User Guide

Clients

EGVP version 2.9.0.2

Document version 1.5

(last amended May 04th 2015)

http://www.egvp.de/

Table of contents

1 Legal information and further notices 4

2 About this manual 5

3 Requirements 6
3.1 Organisational requirements 6
3.2 Technical requirements 6
3.3 Usage notes 10

Valid characters to fill in the business card 10
3.4 Further operational environments of the EGVP 12
3.5 Information on technical background 14

4 Installation guide 15
4.1 Installation with JNLP 15
4.1.1 Installation of the Java Runtime Environment 15
4.1.2 Setting up Java 15
4.2 First start of the JNLP 18
4.3 Java Web Start 19
4.4 Java Web Start security warning 20
4.5 Java terms of licence 20
4.6 Starting the application 22

5 User interface 25
5.1.1 The P.O.box bar 26
5.1.2 The message area 27
5.1.3 The tab bar 31

6 Scenarios 33
6.1 P.O.box handling 33
6.1.1 Establish a P.O.box 33
6.1.1.1 Transfer of an existing identity of the directory service S.A.F.E 33
6.1.1.2 Tab business card 34
6.1.1.3 Entry of basic settings 36
6.1.2 Open a P.O.box 45
6.1.3 Delete a P.O.box 46
6.1.4 Close P.O.box 46
6.1.5 Edit P.O.box 46
6.2 Use of the P.O.box 47
6.2.1 Settings 47
6.2.2 E-mail notification 47
6.2.3 Status report preferences 48
6.2.4 Create new certificate 51
6.2.5 Changing the P.O.box certificate 51
6.2.6 Import preferences 3rd party 52
6.2.7 Import without exchange folder ("dynamic data transfer") 52
6.2.8 Export preferences 53
6.2.8.1 Inbox and sent messages 53
6.2.8.2 Archive 54
6.2.9 Send automatically 56
6.2.10 Receive automatically 57
6.2.11 Delete automatically 57
6.2.12 Address book 57
6.2.13 Subsequent certificate verification 58
6.3 Information regarding the P.O.box 58

6.3.1 Menu Server 58
6.3.2 Menu "?" 59
6.4 Create messages 59
6.4.1 Create a message with the message dialog 59
6.4.1.1 Storing the message in the outbox 62
6.4.1.2 Instant sending 62
6.4.2 Create a message using the 3rd party import (generic import interface) 64
6.5 Address book 64
6.5.1 Select message addressee using the address book 64
6.5.2 Tab "Users" 65
6.5.3 Tab Favourites 68
6.6 Working with messages 71
6.6.1 Send messages 71
6.6.2 Receive messages 72
6.6.3 Handling messages 74
6.6.3.1 Functions from the menu 74
6.6.3.2 Functions from the context menu 76
6.7 Additional functions 79
6.7.1 Debug mode de-/activate 79
6.7.2 Re-enable disabled dialog boxes 79
6.7.3 Quit 79
6.7.4 Agreement to changed privacy policy 79
7 Reports 81
8 Explanations to the inspection sheet 83
9 Information about error messages and alerts 85
10 Table of figures 86
Appendix 1: How to fix problems with the print option in the context menu using Windows 88
Appendix 2: How to uninstall the EGVP application 90

1 Legal information and further notices

Although this product documentation was written to the best of our knowledge and with reasonable care, errors and inaccuracies cannot be totally excluded. Legal or other liability for inaccurate information and their consequences cannot be assumed. The information given in this product documentation reflects the current state of development and can be changed without further notice. Future editions can contain additional information. Technical und typographic errors are corrected in subsequent editions.

This user guide as well as all copyright capable materials that are sold along with this product is copyright protected. All rights are reserved by Governikus GmbH & Co. KG, Bremen, (Governikus KG).

It is prohibited to copy or otherwise reproduce copyright capable materials without previous agreement. For legitimate users of this product this right is granted within the contractual terms. All copies of this user manual must bear the same notice of copyrights, as does the original, regardless whether the complete text or only parts of it are used.

Governikus and Governikus Communicator are registered trademarks of Governikus GmbH & Co. KG, Bremen.

The copyrights of the Java programming language and all other technologies that are freely available at Oracle are registered to Oracle. The copyright for JBoss is registered to Red Hat, Inc. Their terms of trade apply. Other products and technologies that are listed within this product information are possibly trademarks of further owners and must be obeyed respectively.

2 About this manual

Primary target of the user guide is, to offer you information and explanation about installation, functionality, and usability of the electronic court and administration mailbox (**E**lektronisches **G**erichts- und **V**erwaltungs**p**ostfach EGVP). Furthermore this document is intended to help you with any questions or problems you may have using the application.

Chapter 3 names system requirements, which are necessary for using the electronic court and administration mailbox (EGVP). Chapter 4 contains a step by step description of the installation and the start of the EGVP. The user interface with all of its contents is described in detail in chapter 5. In chapter 6 different scenarios and the handling of post boxes is described as well as the handling of messages. Chapters 7 and 8 explain the different protocols created by the EGVP and their evaluation. Chapter 9 contains a short instruction, on how to handle error messages.

3 Requirements

The EGVP is a Java application and has to be loaded with Java™ Web Start from an Internet server. It is also possible to use an installer that will update the software in the same way as Java™ Web Start. Data is exchanged as message between clients, courts, and administrations. Clients, courts, and administrations can be sender as well as addressee.

3.1 Organisational requirements

Please register your EGVP copy after installation via a directory service. This process is automatically started when the data entered in the business card is transferred to the directory service. You are inscribed in the central address book and your address data is selectable as addressee for messages. All clients can only address courts and administrations.

All data belonging to a message is displayed within the EGVP. It can be signed and is sent to an OSCI Manager. The OSCI Manager verifies the signature, creates an inspection sheet, and holds the message in store for the addressee. The message can be received in OSCI format with the addressee's EGVP. All communication follows this process. The corresponding OSCI Manager is integrated by the application.

3.2 Technical requirements

Hardware

For using the EGVP a computer with at least 512 MB RAM main memory and a 1 GHz CPU is required. Additionally the Governikus KG recommends 2 GB RAM main memory, a 2 GHz CPU and 1 GB of free disk space, and at least a DSL Internet connection. The display's resolution of at least 1024x768 pixels is recommended. The font size has to be set to "normal". If necessary a smartcard and a card reader must be at hand.

Supported operating systems

The following operating systems are supported:

- openSUSE 12.x
- Windows XP
- Windows Vista
- Windows 7, Windows 8

Attention:

On systems with 64-bit Java, attachments and messages cannot be sent via e-mail by using the application. Also, the debug mode is concerned by this restriction. If required, please create e-mails with your e-mail-client and add attachments or the logging output manually.

In order to do this, please copy the content from the Java console. The console is shown by using the Java Control Panel (Tab "Advanced", Settings: "Java Console").

Note:

Windows XP SP3 support with Windows™ security updates ended April 8th 2014. As long as no security vulnerabilities emerge Windows XP SP3 can be used until the Governikus KG will officially discontinue it for Governikus products. The Governikus KG recommends upgrading the Windows operating system.

Browser

To display the EGVP-Website and to launch the download a web browser is required.

Java Runtime Environment

A Java Runtime Environment (JRE) is mandatory. In general the JRE is part of the browser and installed automatically. In case the JRE does not exist you can download the currently recommended version from http://www.egvp.de or the website of an affiliated court or administration. To start the application from a website Java Web Start (JWS) is required. It is installed automatically with the installation of the JRE.

The EGVP currently supports the following JRE version:

- JRE 1.7_x (min. 1.7.0_11, tested with version 1.7.0_51)
- The recommended Version is 1.7.0_79.
- JRE 1.8_x (basically tested with 1.8.0_45)

For branch JRE 1.6_x please see attention box below.

Oracle continually develops the JRE, closes security vulnerabilities, and adjusts problems, which might not have been in question at the time of testing. Therefore, we recommend using the current JRE version provided by Oracle.

Attention:

Oracle stopped the support of Java 6 as of March 2013 and will not provide any openly available security patches from this date on. It is possible that this fact will affect the high required security against

	prospective threat for a signature application component. As long as there will not be any security holes, it is allowed to use Java 6 for EGVP. Anyhow we strongly recommend switching to Java 7 immediately. The following version of EGVP will no longer support Java 6.

	Note: Information on current problems caused by Java can be found on http://www.egvp.de/ or http://www.governikus.com/.

	Attention: Problems while starting the application may occur if different bit-versions of Java Runtime Environment (JRE) and Java Web Start are installed. Please make sure JRE and Java Web Start are installed in the same bit-version either 32-bit or 64-bit.

The supported operating systems combined with the supported JRE are listed in the following table.

Operating systems	**Version: JRE 1.6.0**
openSUSE 12.x	at least 1.6.0_41 (not recommended) at least 1.7.0._11
Windows XP	at least 1.6.0_41 (not recommended) at least 1.7.0._11
Windows Vista	at least 1.6.0_41 (not recommended) at least 1.7.0._11
Windows 7, Windows 8	at least 1.6.0_41 (not recommended) at least 1.7.0._11

Table 1: Supported operating systems in combination with the JRE

Necessary access rights for installation, update, and business

Certain access rights are required on the computer. For the installation of Java Runtime Environment/Java Web Start and the first installation of the EGVP you need administrator rights for your computer. Subsequent updates only require normal user rights (read-/write access). The following table shows the different rights, which are necessary for each process.

Process	Read-/Write access
Java installation or update	Depending on the operating system (administrator rights)
First installation update	Java folder (administrator rights)
	User directory
	target directory for the local EGVP P.O.box
	Java preferences (registry of Windows systems)
operational use	User folder
	Folder for the local EGVP P.O.box
	Folder “bremen online services” / “Governikus KG” under “documents and settings” (Windows XP) or ProgramData (Windows Vista, 7, 8)
	Java preferences (registry of Windows systems)
	Defined export folder for messages to export from the EGVP P.O.box.
	Defined import folder and folder for 3rd party interface for messages to import into the EGVP P.O.box

Table 2: Access rights for installation and operation of the EGVP

Please ask your administrator on the first installation if necessary.

Use of smartcards

In legal relations documents usually have to be signed with a qualified electronic signature. Hence, you need a smartcard of a trust centre, which is suited for qualified signatures. The EGVP is not limited to certain smartcards but supports the most German smartcards that enable at least qualified electronic signatures. A list of smartcards whose signature-, certificate-, and request-formats are currently supported by EGVP is located at www.egvp.de or on the web pages of respective courts or administrations of justice. Please request the signature level and possible further requirements needed in respective administrative procedures at courts and administrations.

If you intend to use a smartcard a smartcard reader has to be connected to the computer. A listing of all currently supported smartcard readers is available at www.egvp.de or at the web site of affiliated courts or administrations under "Technical requirements".

Attention:

For generating qualified digital signatures, only smartcard readers must be used that are confirmed according to the German Digital Signature Act (Deutsches Signaturgesetz (SigG)) and whose confirmation is published by the Federal Network Agency (Bundesnetzagentur (BNetzA)). With release of this application only the appointed

	smartcard reader met these requirements. This application also supports smartcard readers that allow or are not (yet) confirmed. If you use such a smartcard reader, you are using this application not as a signature application component with which qualified digital signatures can be created.

3.3 Usage notes

Establish a P.O.box

The P.O.box is to be installed on a local computer because network access depends on transfer rates and other factors which are not influenced by the EGVP. Low transfer rates and special configurations of the EGVP can result in slow responses of the application.

When installing the P.O.box you have to make sure it is installed on the highest level of the hard drive because otherwise problems with saving attachments and folders with more than 255 characters can occur under Windows. Please mind that probably not the entire directory path is displayed. Furthermore we recommend not exceeding a file name length over 60 characters because they also extend the directory path.

Valid characters to fill in the business card

To complete the business card the following regular expressions are allowed:

- Field "phone number":

  [+()-/0-9]{2,}

  This means:

  - All numbers
  - The special characters +()-/
  - At least 2 characters

  This allows for example to enter "+49 (421) 20495-60"

  - Field "E-mail":
    - [A-Za-z0-9.!#$%&'*+\\-/=?^_`{|}~]{2,}@[\\w.\\-_]{2,}\\.[a-zA-Z]{2,6}
    - This allows the entry of e. g. "info@governikus.com".
  - All additional fields:
    - [\\w &'()+,\\-./\\p{InLatin-1Supplement}\\p{InLatinExtended-A}]{2,}
  - This means that the entry of the following characters is allowed:
    - All characters of the alphabet (upper and lower case)

- All numbers
- All umlauts (upper and lower case)
- The special characters &`()+-.,/§
- Blanks

The minimum length of an entry is two characters. A normal or hard space (Alt-255) is not allowed for the beginning or end of an entry.

Scanning of attachments

We recommend scanning documents that are intended to be sent as an attachment in PDF format with a point density of 300 DPI and a colour density of 1-Bit (black/white) in order to minimise the file size. Big attachments slow down the message transfer.

Scan first with the lowest recommended colour depth for the appropriate template in order to test your settings. Compare the result with the original due to readability and visibility. If you are not comfortable with the result, choose a higher quality of the settings.

If there are single documents which need a higher quality than the recommended settings will display (e. g. graphics, documents with shades, official seals or stamps), scan these documents separately with a higher colour resolution/colour depth and create a separated file. By using the PDF format it is possible to assemble the files to one document - dependent on the software which is used.

Use ZIP archives with bigger file attachments in order to compress files. Ensure that the archive contains no other ZIP files or directory structure. Avoid scanning documents which exist already in a digital format. Prove if the digital document with an appropriate signature is alternatively better for dispatching. Moreover, it is recommended - if this technical possibility is available - to convert scanned PDF files into a searchable format via OCR text recognition.

Allowed file types

Information about file types, which can be sent as attachments to courts and administrations can be found in the corresponding ordinances of each state (see also www.egvp.de)

Use of special characters for attachments and content data

The following characters are accepted in attachments and content data within the EGVP:

- all characters of the alphabet (upper and lower case)
- all numbers
- special characters ! § $ % ( ) = , . - _ + # ' @
- blanks

Naming of attachments

Please do not attach any files of the same name as content data. Usually messages created with the EGVP contain content data with the following names: "nachricht.xml", "nachricht.xsl", "visitenkarte.xml", and "visitenkarte.xsl".

Note:

If you intend to send a message of XJustiz, please attach the according file using the identifier "xjustiz_nachricht.xml". This way, the message conforms to the OSCI transport profile for XJustiz.

Write-protected attachments

Please make sure that you only send attachments, which are fully readable and are not read and/or write protected.

Transfer limitations

The default limit for attachments is 30 MB and 100 files. As addressee you have to ensure that you are able to receive messages of this size. Also mind the size limits when sending messages.

Size limitations of the P.O.box

With a maximum of 1000 messages within a post box (meaning in-, out- and sentbox together) and post box dimension of 2 GB per post box the EGVP should operate with an adequate speed. Exceeding these limits may result in reduced performance.

Size restrictions for favourites

The number of favourites is limited to 100.

Further processing of messages

Messages, which have been sent or received with the EGVP can be transferred to the file system by the "Export" function or can be moved via drag and drop (Windows only) from the user interface. From the file system the data of the entire message can be processed. Manual access to data of files within the OSCI folder (location of all messages in the file directory) can result in malfunctions of the EGVP. Therefore no support is guaranteed if manipulations of the file system in the OSCI folder have occurred.

3.4 Further operational environments of the EGVP

Communication of the EGVP within a network

EGVP communicates via HTTP. Therefore the HTTP methods GET, HEAD and POST are used. The TCP ports depend on the configuration of the server. Usually these are the pairs 80/443 and 8080/8443. Authenticating proxies with the schemes Basic and NTLM are supported. When using Java Web Start two password entries are necessary. The reason is

that applications of the Governikus KG do not contain any authentication information but have to request them as well.

If a proxy or firewall filters the download of JNLP and JAR files on application level, it has to be allowed. The following MIME types may not be filtered:

- multipart/related for OSCI
- application/x-java-jnlp-file for download of JNLP descriptors
- application/x-jar for downloading the JAR files
- binary/x-java-serialized for the communication with the directory service

The transport of the OSCI messages uses the HTTP method POST. If a proxy is used the maximum size of POST-requests has to be adjusted to the double size of the maximum size for attachments (60 MB). The default configuration for most proxies is chosen in a way that only small sized files (e. g. 1 MB) can be sent. If necessary the time-out values of the proxy have to be extended as well, if sending larger messages is necessary.

Using EGVP in a network environment

The P.O.box is to be installed on a local computer because the access from a network environment depends on transfer rates and other factors which are not influenced by the EGVP. Low transfer rates and special configurations of the EGVP can result in slow responses of the application.

Please mind the following when using the EGVP in a network environment:

- The user has to have reading and writing rights for the OSCI directory.
- The user may not be limited for the transfer of data within the network.
- The simultaneous access of 3rd party software to the data in the OSCI directory has to be avoided.

Before defining the message directory please mind the following:

- Who is going to use the EGVP? Do you want to share access with colleagues?
- Which computers will operate the EGVP? Is the message directory on the local computer or shall it be available within the network?
- How is renaming of the directory avoided? Which section of your hard drive or file server is not moved or renamed in the future?

If all users shall use a central P.O.box the message directory has to be the same for all users. Therefore you have to find an internal agreement on which directory is used. Please ensure that all users have the required user rights to access the directory.

Support of terminal servers

The Governikus card control drive makes use of the PC/SC standard besides accessing to the KAAN-Professional. The standard offers a unique interface to card control drives. The

operating system (e. g. Microsoft Windows or Linux) offers a service for smartcards, which addresses Governikus by using this standard.

The contemporary terminal software has the ability to tell the driver of the card reader (e. g. with the help of virtual USB ports), that the reader is connected to the local computer (terminal server) although it is situated to the workstation of the user.

Attention:

There is no support for terminal servers at present.

3.5 Information on technical background

The Java™ based EGVP assumes a certain Java™ Runtime Environment (JRE).

Activation and deployment is based on Java Web Start (see Oracle page on Java Web Start), which is included in the JRE installation. Java Web Start automatically installs all resources required on the user's computer. Resources provided on the server must be digitally signed. A web server responds to an HTTP request for a JNLP file (**J**ava **N**etwork **L**aunching **P**rotocol) by delivering it (MIME type "application/x-java-jnlp-file jnlp"). The JNLP file specifies required resources for client software. Resources are passed to an executable file that invokes the Java virtual machine (JVM).

All resources are kept in cache. Thus succeeding calls compare the cache's content with resources on the web server's side and download only those parts that have been changed or updated since last download. Hence, the user is guaranteed to always have the most current version and download volumes are minimised.

Furthermore Java Web Start provides enhanced security mechanisms. It explicitly requests access to devices outside the Java context. It verifies integrity of resources in cache via the digital signature. Employed certificates are displayed. If in doubt the user can cancel the operation.

4 Installation guide

This chapter describes step by step installation, setup, and first launch of the EGVP. The delivery normally is performed with so-called JNLP links.

4.1 Installation with JNLP

The Java™ Runtime Environment (JRE) is required for two reasons. EGVP is Java based and needs the Java Runtime Environment to work properly. While installing the JRE, Java Web Start (JWS) is installed as well. Java Web Start connects to the server, stores the installation data, and automatically checks for updates. In case a provided component is newer than the already installed component, it will be updated without further notice, thus the most current version on the computer.

4.1.1 Installation of the Java Runtime Environment

Please ensure that the correct version of Java is installed.

Note:

If you do not know, which JRE version is installed on your system or if any is installed at all, then proceed as follows.

Microsoft Windows systems:

Open the DOS prompt using the Start menu, "Programs" and "Accessories".

Enter the command "java -version" and press return.

Now, the JRE version is displayed or, if not installed, the note "invalid command or file name" will appear.

Linux systems:

Open a shell and enter the command "java -version" and press return.

Now, the JRE version is displayed or, if not installed, the note "Command not found" will appear.

If you do not have a JRE in version 1.6_xx or 1.7_xx, it has to be installed. Please ensure that you have administrator privileges on your work station. If necessary ask the system administrator. Please download the recommended version on your work station and start installation by double clicking the file "jre-1_6_0_xx-xxxxxx.exe". Read and accept the terms of licence and follow instructions of the installation assistant. After successfully installing the JRE, you can install the EGVP.

4.1.2 Setting up Java

In case the correct version is installed, please take the time to configure Java. Therefore you have to launch the Java Control Panel; usually you can find the respective link on the desktop of your workstation, or look for the file „javacpl.exe” and run it.

	Note: All following descriptions and figures were created with Java 6.

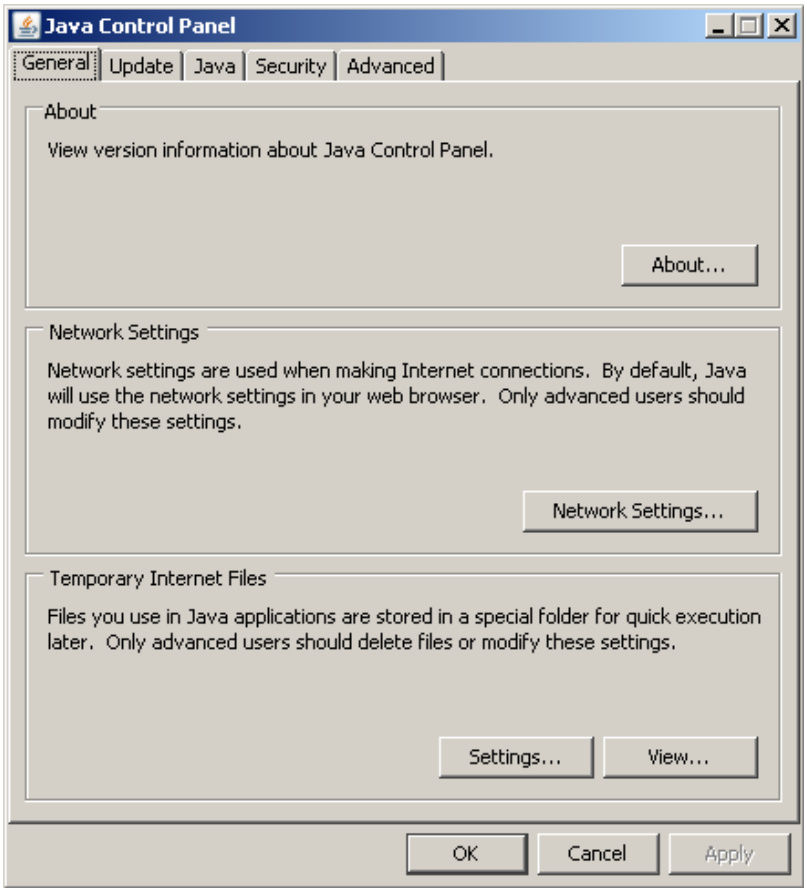
Java Control Panel
General
Update
Java
Security
Advanced
About
View version information about Java Control Panel.
About...
Network Settings
Network settings are used when making Internet connections. By default, Java will use the network settings in your web browser. Only advanced users should modify these settings.
Network Settings...
Temporary Internet Files
Files you use in Java applications are stored in a special folder for quick execution later. Only advanced users should delete files or modify these settings.
Settings...
View...
OK
Cancel
Apply

Figure 1: Java Control Panel of Java 6

Network Settings

Select the "General" tab and press the "Network Settings" button:

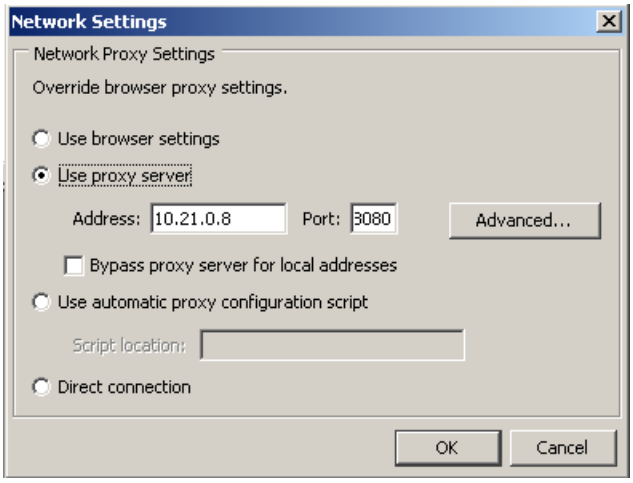

Figure 2: Network settings

Please check the configuration. In case you are using a proxy server, you have to activate the "Use Proxy server" radio button and enter the IP address manually.

	Note: Setting up the proxy server directly ("Use proxy server ") or using the browser settings ("Use browser settings") may have effect on the connection speed.

Click "OK" to save the settings.

Version of Java Runtime Environment

We now recommend checking, whether the correct Java version is activated in the "Java" tab. In the section "Java Application Runtime Settings" click on "View" to open the "JNLP Runtime Settings" dialog:

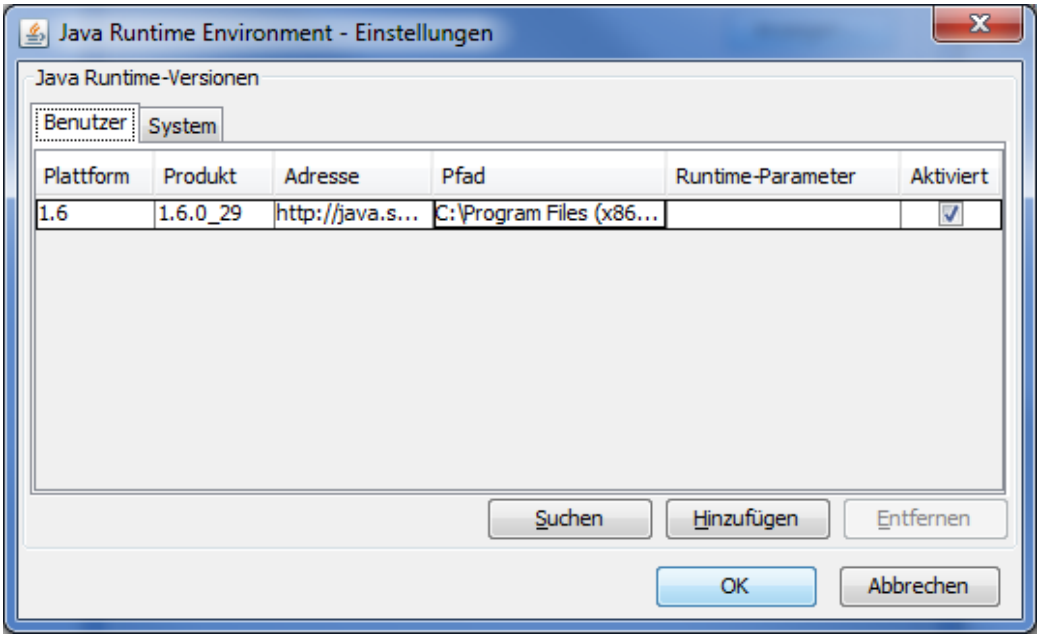

Figure 3: Java application runtime settings

Attention:

It is possible that multiple JREs are installed! If multiple JREs are installed on the computer you have to ensure that Java Web Start uses the correct version which is necessary for the application.

Select the respective check box in the "Enabled" column to activate the correct version. Confirm your choice with the "OK" button.

Logging

To reconstruct potential problems and to find the causes in an adequate time, it is reasonable to record activities in a log file. Therefore select the "Advanced" tab in the Java control panel dialog and open the debugging section by clicking "+".

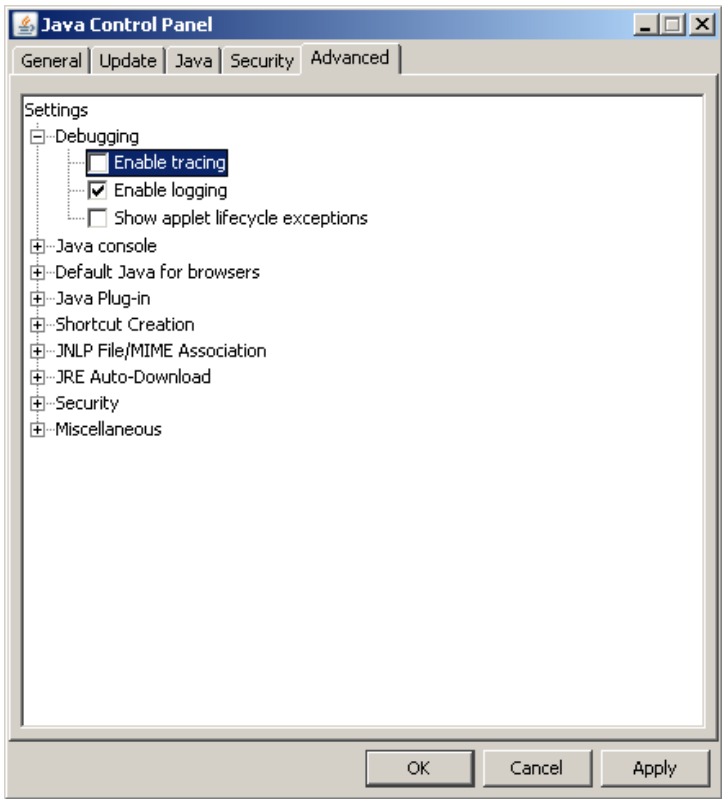

Figure 4: Java Control Panel - Advanced

Activate the "Enable logging" check box and confirm your settings with the "Apply" button. Close Java Web Start.

4.2 First start of the JNLP

The JRE installation is precondition for starting the application. Please mind that an Internet connection has to be established. Start your browser and fill in the application's address. The JNLP-Link is provided on www.egvp.de in the section “Downloads”.

The following or a similar window is displayed:

Figure 5: Java Web Start loads the application

	Note: After installation you can launch the application by selecting the respective item on the Java Cache Viewer. Here, all applications are shown in a selection dialog.

The Java Cache Viewer offers the possibility to create a desktop icon for every previously launched Java application. To create this icon open the view-dialog of the temporary Internet files, mark the respective application and use the context menu to "Install Shortcuts".

4.3 Java Web Start

When starting the first time, the EGVP will be installed together with Java Web Start. Every following start will be handled by JWS, which will connect to the installation server and automatically check for new or updated modules. The download will then start automatically. Depending on data volume, connection speed, and server load the download can last some minutes.

- The amount of downloaded data depends on whether you want to install or update the application. Installation needs more time, because the entire EGVP data has to be loaded. If only an update is executed, there is less data to be downloaded.
- Updates are executed either when launching the application and an online access is available or, in case the connection is established later, e. g. while sending and receiving messages.

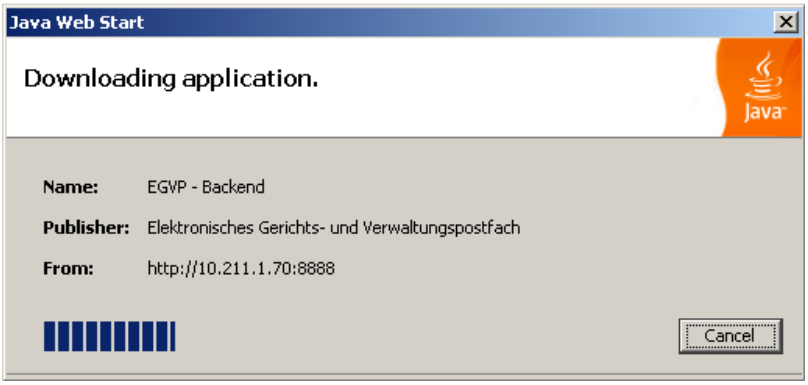

Figure 6: Displaying the download status

4.4 Java Web Start security warning

After the download is finished successfully, a message is displayed. JWS requests access to the local computer and the network. In this safety warning Oracle names the certificate used for signing the downloaded modules and the trust centre, which guarantees the certificates authenticity. The figure below shows a safety warning. The concrete display and message depends on the used JRE version.

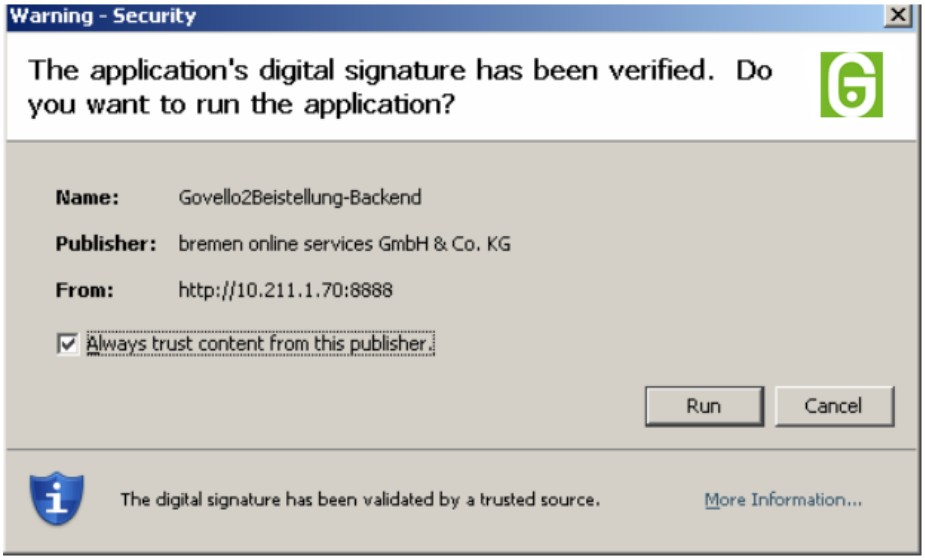
Warning - Security
The application's digital signature has been verified. Do you want to run the application?
Name: Govello2Beistellung-Backend
Publisher: bremen online services GmbH & Co. KG
From: http://10.211.1.70:8888
Always trust content from this publisher.
Run
Cancel
The digital signature has been validated by a trusted source.
More Information...

Figure 7: Safety warning

Oracle safety warning is only displayed with the first download. Click the "Install" button (depending on the version, it can also be referred to as "Complete") to finish the installation and launch the application. The EGVP user interface is displayed.

4.5 Java terms of licence

The first EGVP start presents the Java terms of licence. Please read the declaration and accept it. The following figure shows the text, which can differ depending on the installed JRE version.

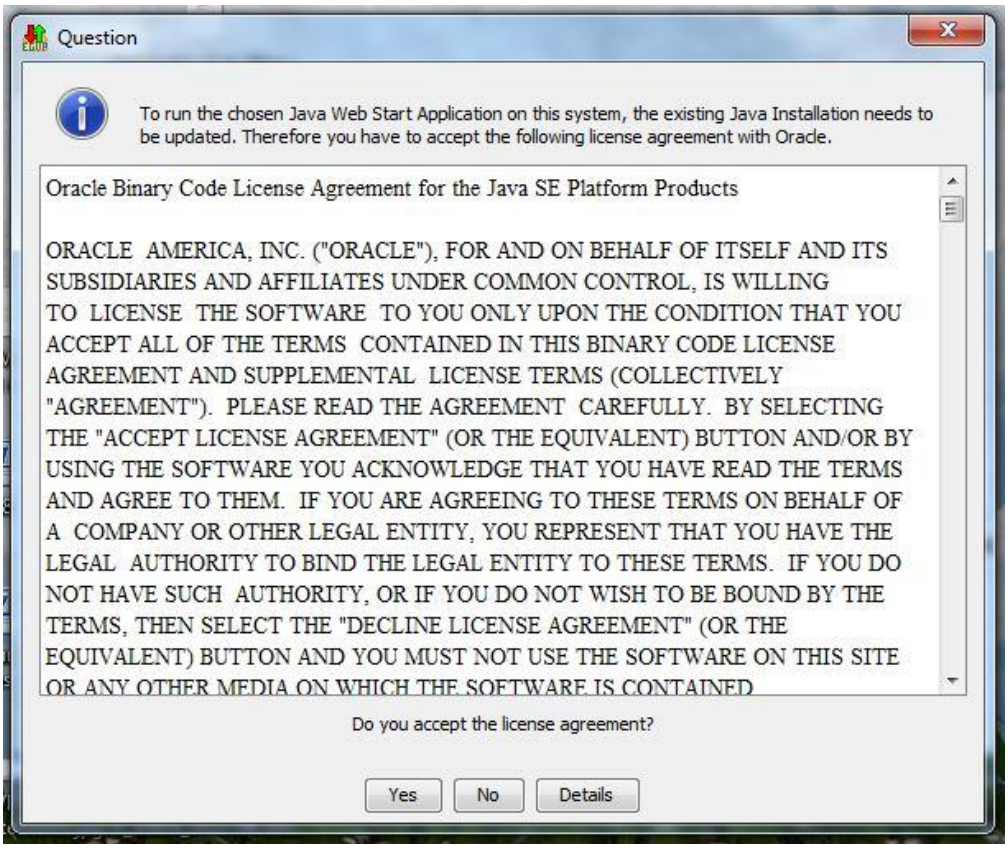
Question
To run the chosen Java Web Start Application on this system, the existing Java Installation needs to be updated. Therefore you have to accept the following license agreement with Oracle.
Oracle Binary Code License Agreement for the Java SE Platform Products
ORACLE AMERICA, INC. ("ORACLE"), FOR AND ON BEHALF OF ITSELF AND ITS SUBSIDIARIES AND AFFILIATES UNDER COMMON CONTROL, IS WILLING TO LICENSE THE SOFTWARE TO YOU ONLY UPON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS CONTAINED IN THIS BINARY CODE LICENSE AGREEMENT AND SUPPLEMENTAL LICENSE TERMS (COLLECTIVELY "AGREEMENT"). PLEASE READ THE AGREEMENT CAREFULLY. BY SELECTING THE "ACCEPT LICENSE AGREEMENT" (OR THE EQUIVALENT) BUTTON AND/OR BY USING THE SOFTWARE YOU ACKNOWLEDGE THAT YOU HAVE READ THE TERMS AND AGREE TO THEM. IF YOU ARE AGREEING TO THESE TERMS ON BEHALF OF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE LEGAL AUTHORITY TO BIND THE LEGAL ENTITY TO THESE TERMS. IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF YOU DO NOT WISH TO BE BOUND BY THE TERMS, THEN SELECT THE "DECLINE LICENSE AGREEMENT" (OR THE EQUIVALENT) BUTTON AND YOU MUST NOT USE THE SOFTWARE ON THIS SITE OR ANY OTHER MEDIA ON WHICH THE SOFTWARE IS CONTAINED
Do you accept the license agreement?
Yes
No
Details

Figure 8: Java terms of licence (example)

Note:

Under Windows Vista and Windows 7 a prompt may notify you that you do not have administrator rights. This prompt can be displayed even though you are logged in as administrator. In this case, you have to modify the user access control. Please proceed as follows:

Windows Vista:

Select "Start" and go inside the "Control Panel".

Choose "User Account" and then "Turn User Access Control on" or off.

The checkbox "Use User Account Control (UAC) to help protect your computer" **must** be unchecked.

Click "OK" to confirm.

Restart your computer for the changes to take effect. Please mind that this change applies for every user. Then, restart the application. After the installation, the security level can be reset to its former state.

Windows 7:

Select "Start" and enter "uac" in the search box.

Press "Enter". "User Account Control User Settings" are displayed.

Move the slider downwards to "Never notify". With this setting, no more warning will appear when changes to the system are made.

Click "OK" to confirm.

Restart your computer for the changes to take effect. Please mind that this change applies for every user. Then, restart the application. After the installation, the security level can be reset to its former state.

Alternative procedure:

In Windows Vista and Windows 7 you can also start EGVP as an administrator for one time after the download is completed. Please do the following:

1. Create a shortcut. Therefore go to "Start" type "javaws -viewer" in the search bar. Confirm your entry with "OK".
2. The Java Cache Viewer opens. Right-click on "EGVP" and select "Create shortcut" from the menu.
3. Quit the Java Cache Viewer. The shortcut can be found on your desktop.
4. Right-click on the shortcut and select "Run as administrator". The application opens.

4.6 Starting the application

After the installation process you are now presented the application. A start screen is displayed. This splash screen is always displayed while starting the application.

Terms of use

When launching the EGVP the first time, a window with two functions is shown: First you are informed about the current terms of use of EGVP. The second function defines the storage location of messages created with the OSCI based communication.

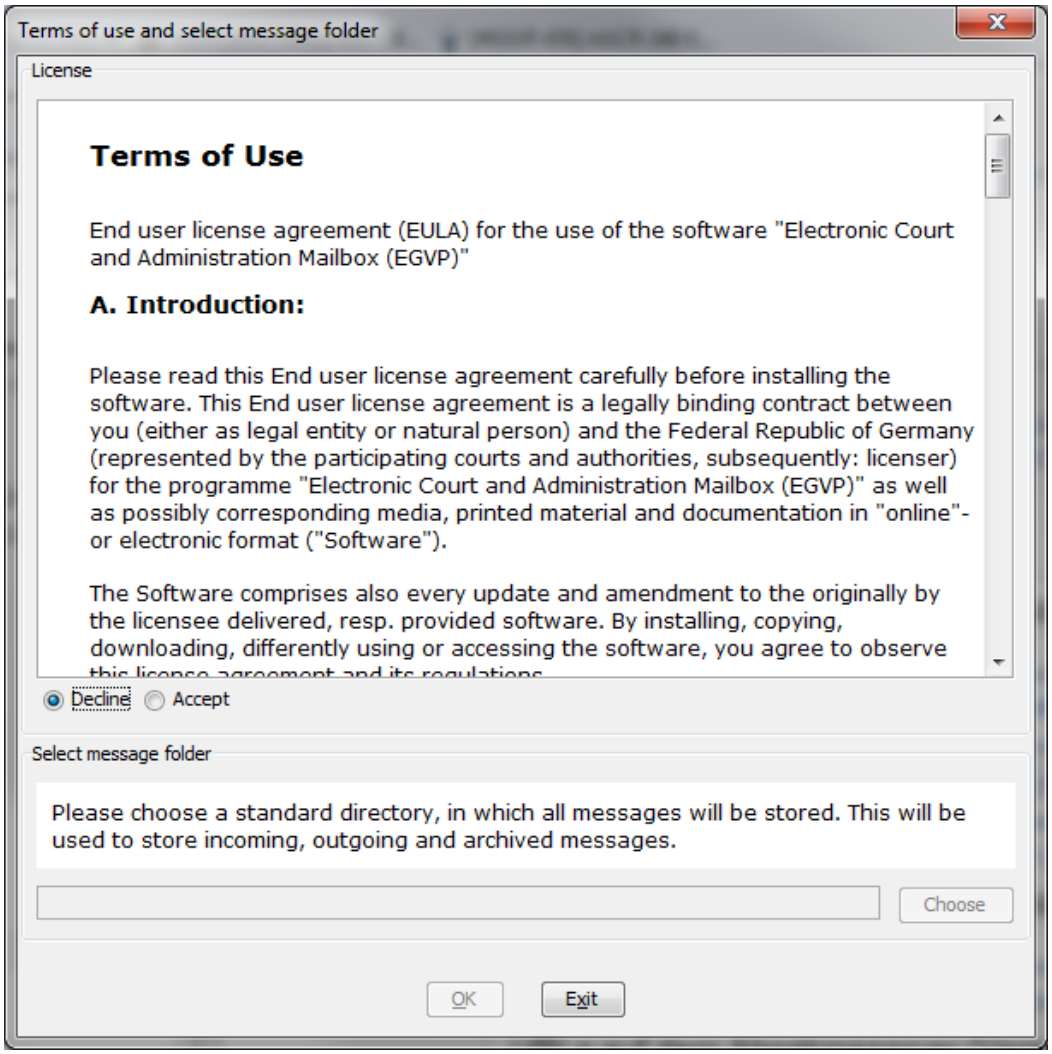
Terms of use and select message folder
License
Terms of Use
End user license agreement (EULA) for the use of the software "Electronic Court and Administration Mailbox (EGVP)"
A. Introduction:
Please read this End user license agreement carefully before installing the software. This End user license agreement is a legally binding contract between you (either as legal entity or natural person) and the Federal Republic of Germany (represented by the participating courts and authorities, subsequently: licenser) for the programme "Electronic Court and Administration Mailbox (EGVP)" as well as possibly corresponding media, printed material and documentation in "online"- or electronic format ("Software").
The Software comprises also every update and amendment to the originally by the licensee delivered, resp. provided software. By installing, copying, downloading, differently using or accessing the software, you agree to observe
Decline
Accept
Select message folder
Please choose a standard directory, in which all messages will be stored. This will be used to store incoming, outgoing and archived messages.
Choose
OK
Exit

Figure 9: Terms of use

Please read the terms of use and accept the conditions to use EGVP.

Select message folder

You now have to set the message folder's location.

	Attention: The folder can only be defined once with the first launch of the application. Changing the folder after the event is hardly possible.

Please consider thoroughly before choosing the message folder, how you can avoid a change of the respective path to the folder. Are there parts on your hard disk where you can be sure, that they neither will be adjusted nor renamed in the next time? We recommend

choosing a high level directory to create the main message folder, e. g. `c:\OSCI-messages`. The application generates a sub-folder `osci_governikus` and stores all messages and attachments in this subdirectory.

- Click the "Select" button.
- Select and possibly create a directory for your P.O.box. Change to the chosen folder and complete with the "Select" button.

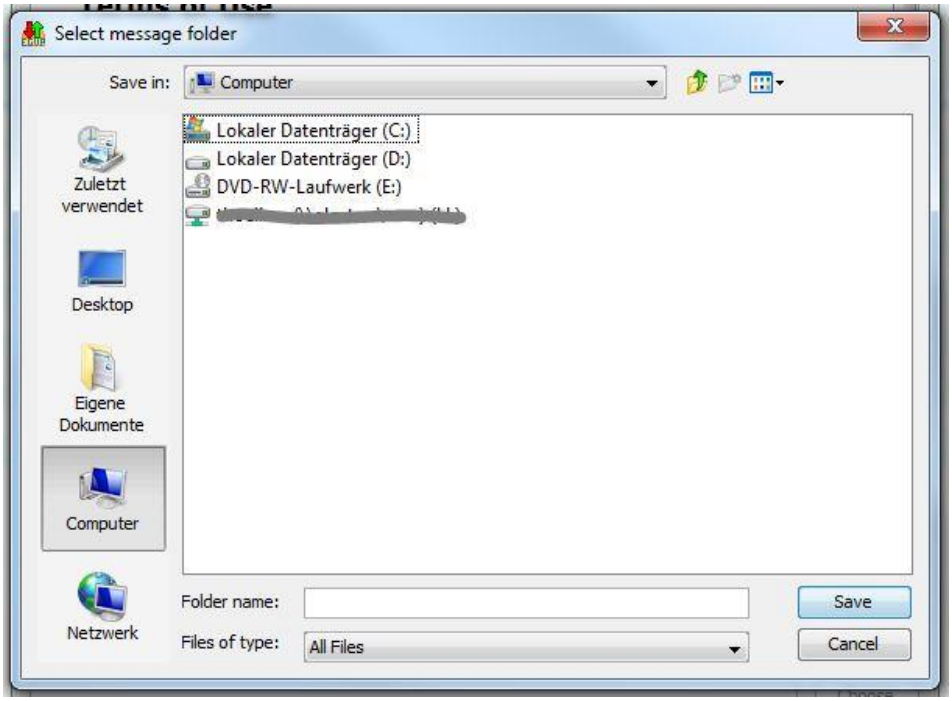

Figure 10: Select message folder

After your selection the window "Terms of use" and "select message folder" is back in display. Check the shown directory for the message folder and press the "OK" button. To create a new EGVP P.O.box refer to chapter "P.O.box handling".

5 User interface

Those who are familiar with e-mail programs will easily understand the basics of the application. The user interface offers a management dialog for sent and received messages. If required more dialogs open after respective user activities, e. g. the login window when launching the application, a dialog to build new messages and another to define the individual P.O.box preferences. The elements of the management dialog are the toolbar, the P.O.box bar, the message area, and the tab bar.

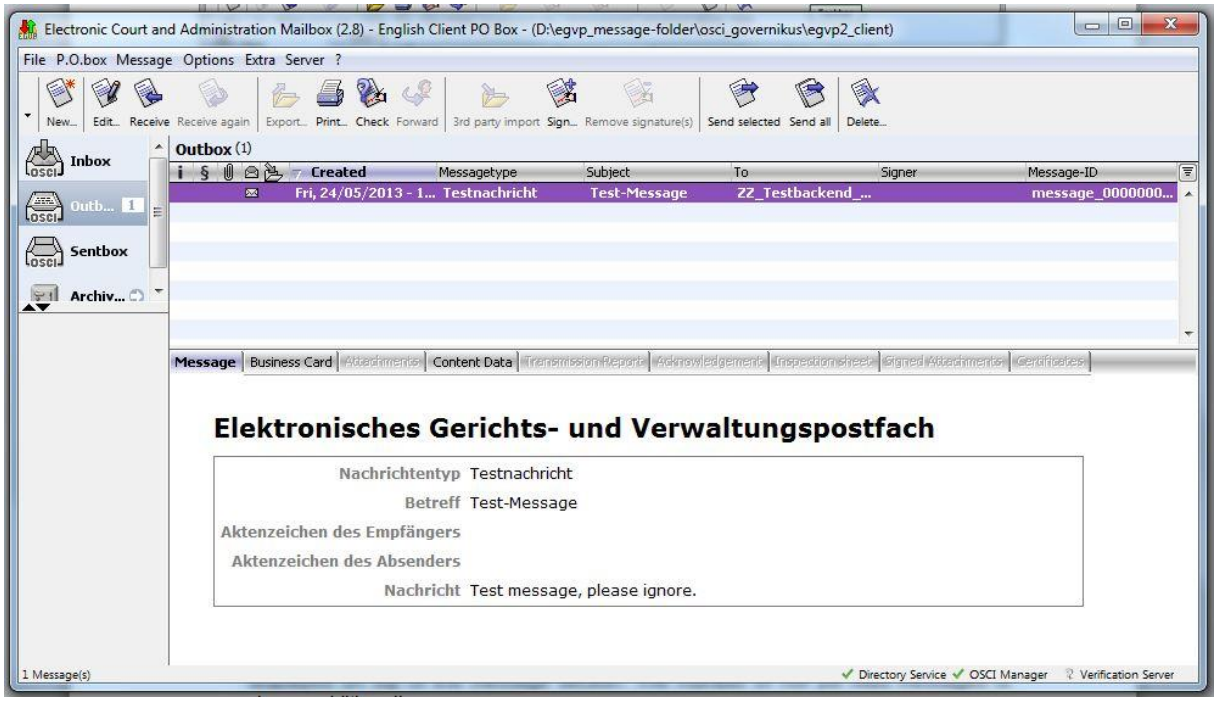
Electronic Court and Administration Mailbox (2.8) - English Client PO Box - (D:\egvp_message-folder\osci_governikus\egvp2_client)
File P.O.box Message Options Extra Server ?
New... Edit... Receive Receive again Export... Print... Check Forward 3rd party import Sign... Remove signature(s) Send selected Send all Delete...
Inbox
Outb... 1
Sentbox
Archiv...
Outbox (1)
Created Messagetype Subject To Signer Message-ID
Fri, 24/05/2013 - 1... Testnachricht Test-Message ZZ_Testbackend_... message_0000000...
Message Business Card Attachments Content Data Transmission Report Acknowledgement Inspection sheet Signed Attachments Certificates
Elektronisches Gerichts- und Verwaltungspostfach
Nachrichtentyp Testnachricht
Betreff Test-Message
Aktenzeichen des Empfängers
Aktenzeichen des Absenders
Nachricht Test message, please ignore.
1 Message(s)
Directory Service OSCI Manager Verification Server

Figure 11: User interface (example)

The main dialog elements of the user interface are:

- **Menu bar**: With the menu bar you manage the user interface. The menu items allow the user to quit the application or to change settings.

- **Tool bar**: Use the toolbar to create, edit, and handle messages. The same functions are available with the "Messages" menu.

- **P.O.box bar**: The P.O.box bar is located at the left hand side of the user interface and allows selecting the "Inbox", the "Outbox", the "Sentbox", and the "Archive". The selected box is highlighted in colour and the name of the respective post box is displayed on top of the message section. The number of not yet read messages is shown additionally.

- **Message area**: The message area contains the major data of created, sent, and received messages. Depending on the shown post box, different information is displayed in a table. You may change the displayed columns by right-clicking the heading.

- **Tab bar**: Different tabs display all information available for the respective message. Select a row in the message table to choose a note and click in the lower half of the dialog on the tab you want to see. Keep in mind, that depending on the active P.O.box only certain tabs are enabled. The description of the several tabs is described in the chapter "The tab bar".

- **Status section**: The current status of sending and receiving processes is shown here.

5.1.1 The P.O.box bar

Inbox

To display all received messages click the "Inbox" button. The message area shows a table with default columns:

- "Verification result of the OSCI message due to the inspection report", "Signature level", "Attachments", "(un)read", "Replied/Forwarded", "Exported", "Imported", "Arrival at server", "Message type", "Subject", "From", "Signer" and "Message-ID".

Additionally you can select the columns:

- "Receiver reference number", "Sender reference number", "Organisation Sender", "Sender-ID", "Zip code Sender", "City Sender", "E-mail Sender" and "Phone Sender".

You may change the displayed columns by right-clicking the heading. The tab bar below has the tabs:

- "Message", "Business card", if existent "Attachments", "Content Data", "Inspection Sheet", if existent "Signed Attachments", and "Certificates" enabled.

Outbox

To see, which messages are ready to send, click the "Outbox" button. The table in the message section displays the default columns "Message signature status", "Signature level", "Attachments", "(un)read", "Imported", "Created", "Message type", "Subject", "To", "Signer", and "Message-ID". Additionally you can select the columns "Sender reference number", "Receiver reference number", "Organisation Receiver", "Receiver-ID", "Zip code Receiver", "City Receiver", "E-mail Receiver" and "Phone Receiver". You may change the displayed columns by right-clicking the heading. Active tabs are "Message", "Business card", if existent "Attachments", "Content Data", and "Certificates". In case the message is marked red an error during import or sending occurred.

Sentbox

To display all sent messages click the "Sentbox" button. The message area will now show a table with the default columns "Not fetched", "Signature level", "Attachments", "(un)read", "Exported", "Arrival at server", "Message type", "Subject", "To", "Signer", and "Message-ID". Additionally you can select the columns "Sender reference number", "Receiver reference number", "Organisation Receiver", "Receiver-ID", "Zip code Receiver", "City Receiver", "E-mail Receiver" and "Phone Receiver". You may change the displayed columns by right-clicking the heading. The tab bar below will have the tabs "Message", "Business card", if existent "Attachments", "Content Data", "Transmission Report", "Acknowledgement", and "Certificates" enabled.

Archive

To display all archived messages, click the "Load archive messages"-button. In case the archive is already loaded, click the button "Archive". The message area displays the default columns "Unpacking status", "Signature level", "Attachments", "Source", "Arrival at server", "Message type", "Subject", "From", "To", "Signer" and "Message-ID". Additionally you can select the columns "Sender reference number", "Receiver reference number", "Organisation", "User-ID", "Zip code", "City", "E-mail" and "Phone". You may change the displayed columns by right-clicking the heading.

The tab bar below has the tabs "Message", "Business card", if existent "Attachments", "Content Data", "Transmission Report", "Acknowledgement", " Inspection Sheet ", if existent "Signed Attachments", and "Certificates" depending on the source (incoming or sent messages) enabled.

5.1.2 The message area

Verification result of the OSCI message according to the inspection sheet

This inbox column gives a short overview of the signature and certificate verification result. Possible symbols are:

- All exams have passed with a positive result.
- At least one of the checks could not be accomplished.
- Minimum one of the executed exams passed with a negative result.

	Note: Messages with the verification result "not accomplished" will continuously be verified automatically, to check whether the status has changed. If the re-examination has a positive or negative result, than this will be shown in the verification result as well as in the inspection sheet.

You have to change to the "Inspection Sheet" tab and, if existent, the "Signed Attachments" tab to see more details.

	Note: The verification of signed attachments is executed temporally delayed after the message is completely received and the OSCI message is verified. Thus, the message is displayed in the inbox before the verification of the signed attachments is started. This can result in a later change of the messages verification result, displayed in the message area.

Note:

Opening an embedded document (enveloping signature) is only possible, if the file type is included in the file name. It is not allowed to change the name of the PKCS7 file (e. g. filename.doc.pkcs7).

Signature level (§)

The column signature level will be marked by the paragraph symbol. For every message the designated level of certificate is displayed:

- (Q) stands for a qualified signature level
- (F) advanced signature level

No item means that there is no need to sign the note. The created message cannot be sent unless it is not signed with at least the necessary signature level.

Attachments ( )

This column informs you, if the message contains an attachment.

(Un)read ( )

The envelope will show the read status of the designated note in every post box. An open mailer shows a read and a closed one an unread message. Unread notes are also written in bold.

Information (i)

This outbox column displays the current message status:

- The message is sent or received just now.
- The message still has to be signed according to the designated signature level.
- The message was signed according to the designated signature level
- The message is edited right now.

In the sentbox this column will show you whether the message has been received by the addressee (no symbol) or not ( ).

Note:

With every start of the EGVP the message status is checked and the display is updated. The display can also be updated manually from the context menu "check status"

Export

In case, the message was exported, a blue arrow ( ) is displayed in this column inside the inbox and sentbox.

Import

This column is shown in the inbox and outbox. If a message was imported a symbol is shown here.

- The message was imported
- The message was not imported correctly. The message is also marked red in the message area.

Forwarded

This additional column in the inbox shows whether the message is forwarded.

Server entry (end of receiving)

Within inbox, sentbox, and archive the column "Server entry" with the receiving timestamp (date and time) is displayed. Please note, that this is the moment the message was completed on the OSCI Manager and not the moment of receiving the message in EGVP. This time specification is the same as the one on the inspection sheet as well as the one on the transmission report, the sender will get after transferring to the OSCI Manager.

Note:

The OSCI Manager is the receiving device of the service provider. Thus, the entry at this server is decisive to protect time limits.

By default all messages are ordered by date, meaning the newest messages is in the first row. Click the title of the "Server entry" column to sort the table a- or descending by ID.

Created

Only displayed in the outbox, this column shows the creation time of newly generated messages (not the time, the signature was applied!),

Message type

This column exists in the "inbox", "outbox", and "sentbox" and represents the type of message. The characterisation will help to find messages of a special content or function.

Subject

This column shows the respective contents of the subject. It is available in all post boxes

"From" and "To"

The inbox will show the column "From" with the name of the sender, the other boxes point to the column "To" with the receiver of each message. The archive contains both columns. Click the column title to reorder the table. The data can be sorted by name and first name in a- or descending order.

Signer

The column appears in every post box, showing the signers name for each message. Together with the signer the time of signature is displayed. If a message is signed this is indicated by a symbol in the column "status". Click the table title to sort the data in ascending or descending order.

Message-ID

The OSCI Manager provides a unique identification for every message, shown in the ID column in all post boxes. By default all messages are ordered by date, meaning the newest note is in the first row. Click the title of the ID column to sort the table as- or descending by ID.

Note:

The ID of a message is part of the folder name, build for every received or sent note in the application directory. Compare definition of working directory and OSCI filing within the file system

"Sender reference number" and "Receiver reference number"

These columns display the receivers and senders reference number.

Organisation (Sender or Receiver)

Depending on the post box, this column shows the organisation of the addressee or the sender.

"Sender-ID", "Receiver-ID", and "User-ID"

This column displays the user-ID. In the inbox it is named sender-ID and shows the user-ID of the sender; in out- and sentbox the receiver's user-ID is displayed. The archive shows the sender-ID in incoming and the receiver-ID in outgoing messages.

Zip code (Sender or Receiver)

This column displays the senders zip code in the inbox, the receivers zip code in out- and sentbox and both in the archive, depending on whether the message is incoming or outgoing.

City (Sender or Receiver)

This column shows the name of the city of sender or receiver.

E-mail (Sender or Receiver)

Depending on the displaying post box, this column shows the e-mail address of the addressee or the sender.

Phone (Sender or Receiver)

This column shows the phone number of the respective sender or receiver.

5.1.3 The tab bar

Message

The "message" tab is available in all post boxes and shows the content of each message in the same way it was entered in the message dialog. Therefore sender and receiver in the EGVP are guaranteed to see the note in the exact same manner.

Business card

The tab is available in all post boxes and shows the respective information (name, address) of the correspondent.

Attachments

The tab is available in all post boxes and shows the file names of attachments assigned, created, sent, and received messages. With double-click the associated application (depending on the file extension) is launched and shows the content of each attachment. Additionally it is possible to save a selected attachment in any folder from the context menu. Therefore you only have to select a folder. It is not necessary to name the file.

Content data

All files are shown that are signed with the help of the sign function. These are the real message files. The tab is available in all post boxes.

Transmission report

This tab is available in the "sentbox" and the "archive" and displays the transmission report, containing all information returned to sender, while sending the message to the OSCI Manager. The data are e. g. the point in time, the message arrived at the OSCI Manager.

Acknowledgement

The tab is available in the "sentbox" and the "archive". It is the confirmation of receipt, containing all information returned to sender while sending the message to the OSCI Manager. The data e. g. the point of time, the message arrived at the OSCI Manager.

Inspection sheet

The tab is available in the "inbox" and the "archive" and represents the inspection sheet. With every message you will receive a routing slip created by the OSCI Manager containing the results of the signature and certificate exams.

Certificates

This tab provides a brief overview of all received or sent certificates assigned to the message and is available in all post boxes.

Note:

For every selected massage you can mark a signature certificate in the "Certificates" tab. Use the context menu (right mouse button) to verify its state online at the certification authority. The verification time is pre-selected to the time of receipt on the server (OSCI Manager). However, you can change the verification time. The verification result is displayed and can be saved and printed.

Please mind that the message's verification result in the "Inspection sheet" tab does not change in the process.

For validation the time has to be defined first. By default, this is the time of entry at the OSCI Manager (inbox and sentbox) and the time, when the message was created in the outbox.

Signed attachments

This tab is available if the message contains an attachment, which is signed with PKCS#7. The tab shows the result of the validation. All certificates which have been used to sign the attachments are checked. The result has impact on the status of the entire message.

After finishing the validation of the signed attachments, the verification result of the message is adjusted (first column in the inbox). The verification result is a summary of the validation result regarding the OSCI message and the inspection sheet of signed attachments, following these rules:

- In case one of the validations is "not valid" (red) the status is set to "not valid" (red).
- In case all validations are "valid" the status is set to "valid" (green).
- In case at least one validation is "not defined" the status is set to "not defined" (yellow)

If no signed attachment exists the status is determined from the inspection sheet. A validation is possible for documents, which include the PKCS#7 signature (enveloping signature) or which have the PKCS#7 signature attached (detached signature).

Note:

Opening an embedded document (enveloping signature) is only possible if the file type is included in the file name. The name of the PKCS7 file may not be changed (e. g. filename.doc.pkcs7).

6 Scenarios

This chapter offers information about typical situations while using the EGVP. We will show you how to create a new or edit or open an existing post box. Furthermore you learn to close or delete a P.O.box and to send messages and work with them.

6.1 P.O.box handling

This chapter shows how to create a new or edit or open an existing post box. Furthermore you will learn to close or delete a P.O.box after working with it.

6.1.1 Establish a P.O.box

To create new P.O.boxes follow the next steps:

- Click "New" within the sign-in dialog or choose the P.O.box menu option "New" to create a new P.O.box.

The dialog "Privacy policy" is displayed. Accept the policy for establishing a new post box. Additionally you can view a listing of all participating courts and administrations. You can also define whether the addressee is able to send you messages or not

- Option 1: Communication with creating a P.O.box. Activate this radio button if you wish to establish a personal P.O.box. The addressee can send you legally binding electronic messages. For further information please click on "Details". A window is displayed and shows the "Data privacy statement EGVP".

- Option 2: Communication without creating a P.O.box. Activate this radio button if you do not wish to establish a personal P.O.box. You cannot receive legally binding answers or an electronic acknowledgement. For further information please click on "Details". A window is displayed and shows the "Data privacy statement EGVP".

- Option 3: No agreement to the data privacy policy. If you do not want to choose any of the above options please choose the third option. A use of the EGVP is not possible in this case!

6.1.1.1 Transfer of an existing identity of the directory service S.A.F.E

By choosing the 1st option, there will pop up the following window:

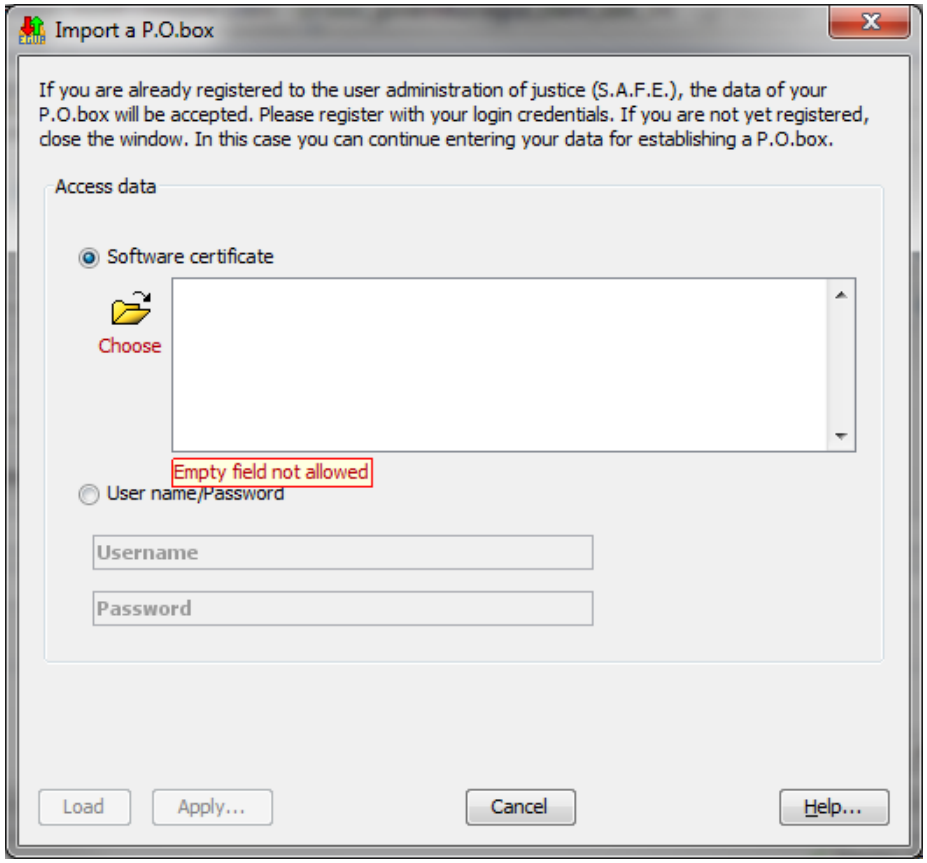
Import a P.O.box
If you are already registered to the user administration of justice (S.A.F.E.), the data of your P.O.box will be accepted. Please register with your login credentials. If you are not yet registered, close the window. In this case you can continue entering your data for establishing a P.O.box.
Access data
Software certificate
Choose
Empty field not allowed
User name/Password
Username
Password
Load
Apply...
Cancel
Help...

Figure 12: Import a P.O. box

If you are already registered to the directory service S.A.F.E. you can use these login credentials for the registration to communicate with EGVP. Select either a software certificate (.p12-key) or a user name/password.

Subsequently you can prove if your data is known by the directory service. If the data is not available on S.A.F.E., an error message will pop up. You have the choice to repeat the entry or to close the window and to establish a new P.O.box (s. 6.1.1.2 Tab business card). If the verification was successful, the existing data on the directory service can be used for the P.O. box of EGVP. Click "Apply" to confirm the operation. You will see the business card where it is possible to complete or to edit the existing data (s. 6.1.1.2 Tab business card).

6.1.1.2 Tab business card

If you are not yet registered to the directory service S.A.F.E., close the window "Import a P.O. box.

After accepting the privacy policy with the 1st option you will reach the "Settings" dialog with two tabs: "Business card" and "Basic settings". First enter all personal information to be sent later with every message to the addressee. Mandatory fields are shown red. Confirm your entries with "OK".

Note:

After accepting the privacy policy with the 2nd option short information is displayed and you will reach the user interface directly. You can now send new messages but are not able to receive any messages.

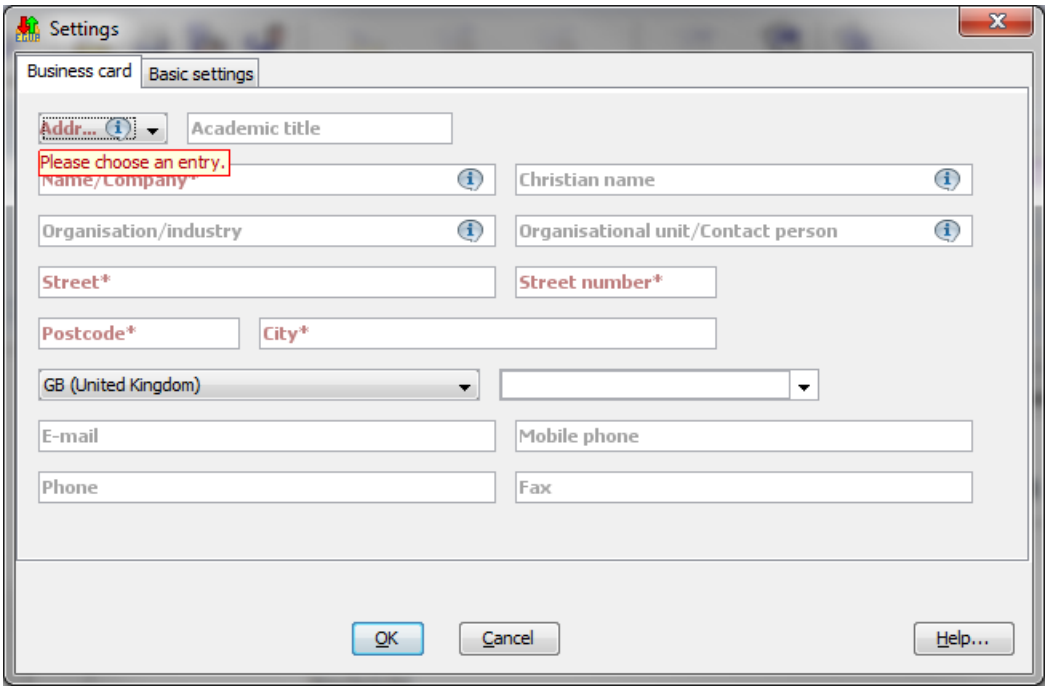

Figure 13: Setting in the tab "business card"

Note:

To complete the business card the following regular expressions are allowed:

- Field "phone number":

  [+()-/0-9]{2,}

  This means:

  - All numbers
  - The special characters +()-/
  - At least 2 characters

  This allows for example enter "+49 (421) 20495-60"

- Field "E-mail":

  [A-Za-z0-9.!#$%&'*+\\-/=?^_`{|}~]{2,}@[\\w.\\-_]{2,}\\.[a-zA-Z]{2,6}

- All additional fields:

  [\\w &'()+,\\-./\\p{InLatin-1Supplement}\\p{InLatinExtended-A}]{2,}

  This means:

  - All characters of the alphabet (upper and lower case)
  - All numbers
  - All umlauts (upper and lower case)
  - The special characters &\`()+-.,/
  - blanks

The minimum length of an entry is two characters.

A normal or hard space (Alt-255) is not allowed for the beginning or end of an entry.

6.1.1.3 Entry of basic settings

Afterwards you have to define a name for your P.O.box in order to distinguish it from other P.O.boxes. The name is shown in the log-in window.

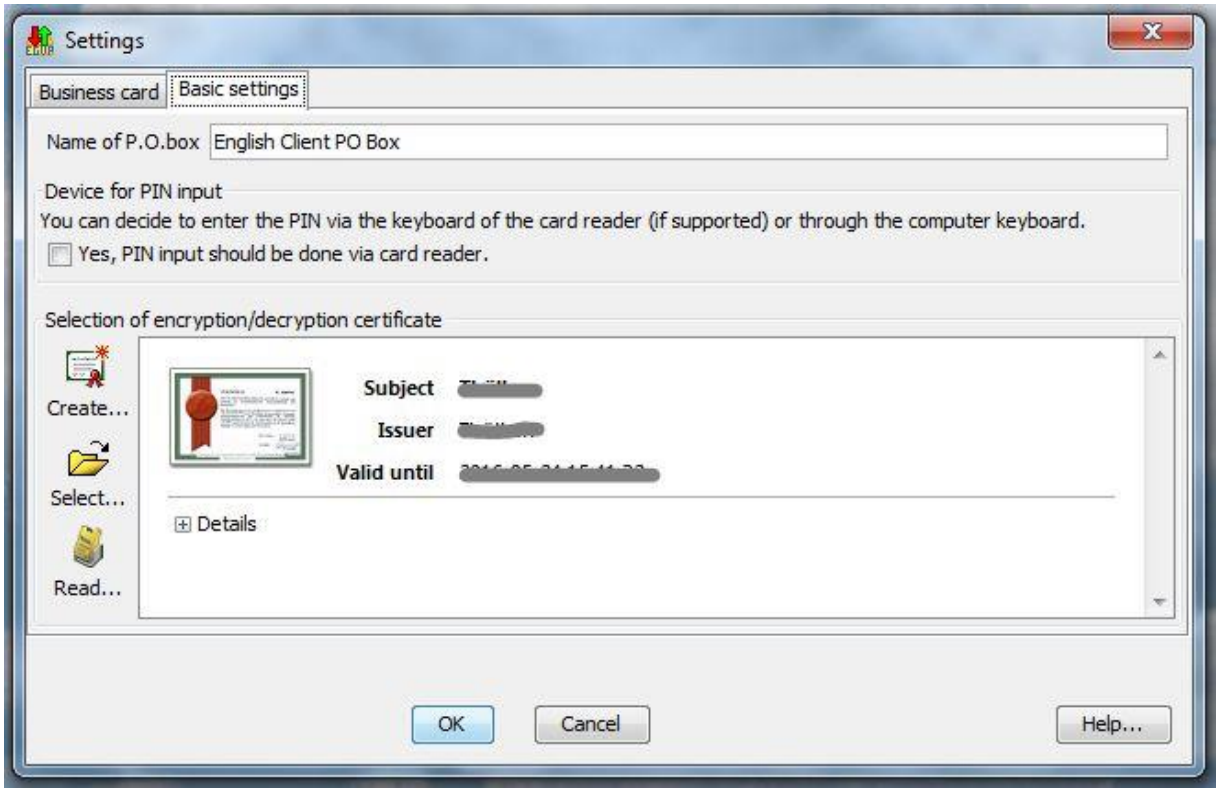

Figure 14: Settings in the tab "business card"

6.1.1.3.1 Selection of encryption/decryption certificate

Every P.O.box needs a certificate that is used exclusively for encryption and decryption but not for signing. The **Governikus KG recommends the use of a software certificate.** You can avoid multiple PIN entries and can create person independent P.O.boxes, which can still be used in case of absence. Please set the kind of ciphering you intend to use and continue:

- self-provided software certificate
- software certificate at hand
- smartcard at hand

Before that, you can already decide whether your PIN-entry is done via the computer's keyboard or with the key pad of the card reader. The PIN has to be at least 4 digits long and may not exceed 20 digits.

Note:

It is strongly recommended to use a software certificate for ciphering in the EGVP!

To save the certificate we recommend to create a sub folder for certificates (in the example on a server, for security reasons saving on an external device is preferable)

```
\Documents and Settings\software certifikates or

<connected server directory>\software certifikates
```

Copy the corresponding file in the defined directory.

Note:

Make sure that the software certificate for establishing your P.O.box is not expired. Establishing a P.O.box with an expired certificate is not possible.

6.1.1.3.1.1 Use of a self-provided software certificate

In case you like to create and use a new electronic signature, click the "Create" button and the "Creation of software certificate" dialog will be displayed.

Note:

This certificate is not intended to sign messages.

You have to define a PIN for the certificate. The PIN must have a minimum of 4 digits and you have to confirm the PIN by entering it a second time. Close the dialog by clicking on "Create".

Figure 15: Create certificate and define PIN

The new certificate has to be saved now. Select the target folder. As file name use the same name you already used for your P.O.box.

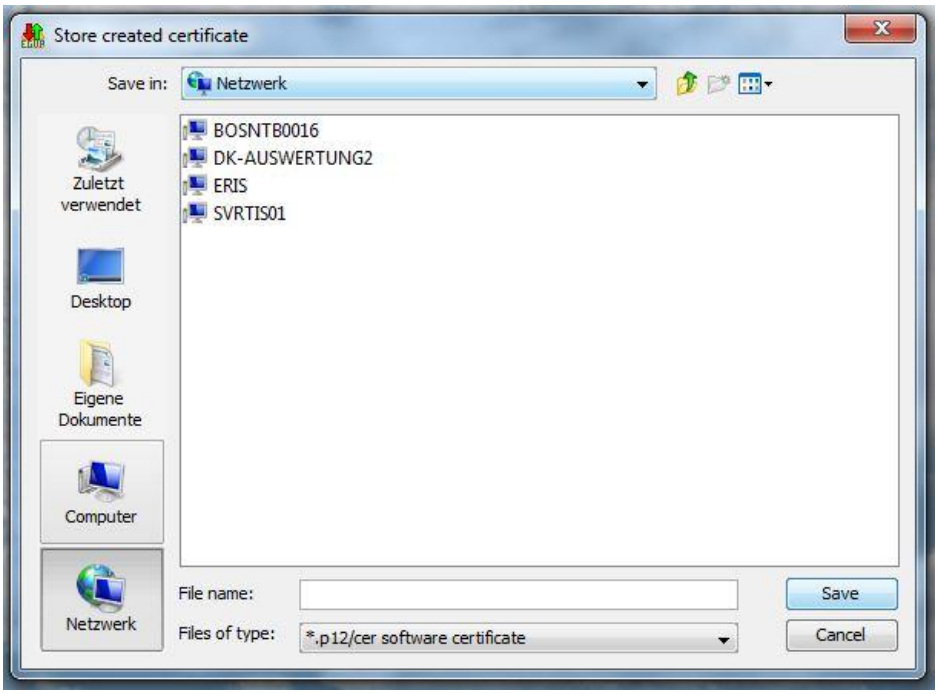

Figure 16: Save certificate

	Note: Without the certificate you cannot access to your P.O.box or your messages. Please store a copy of the certificate at an additional save place to make sure that you can access your P.O.box even if your original certificate gets lost.

You are asked to enter the PIN for the created certificate.

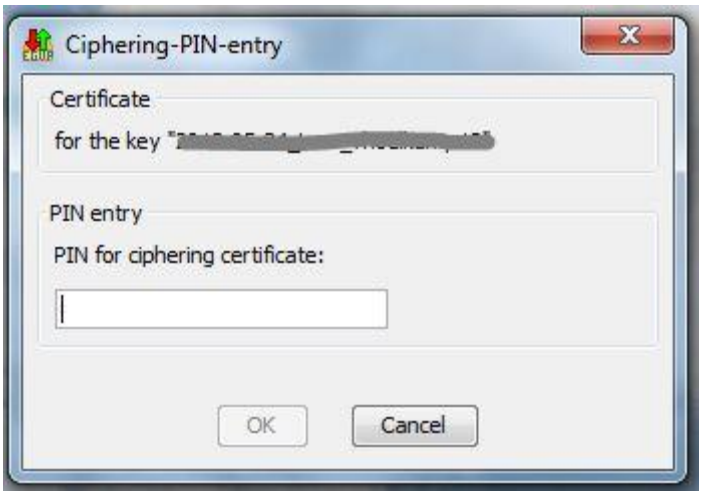

Figure 17: PIN entry

Finally the certificate is shown in the tab "Basic settings".

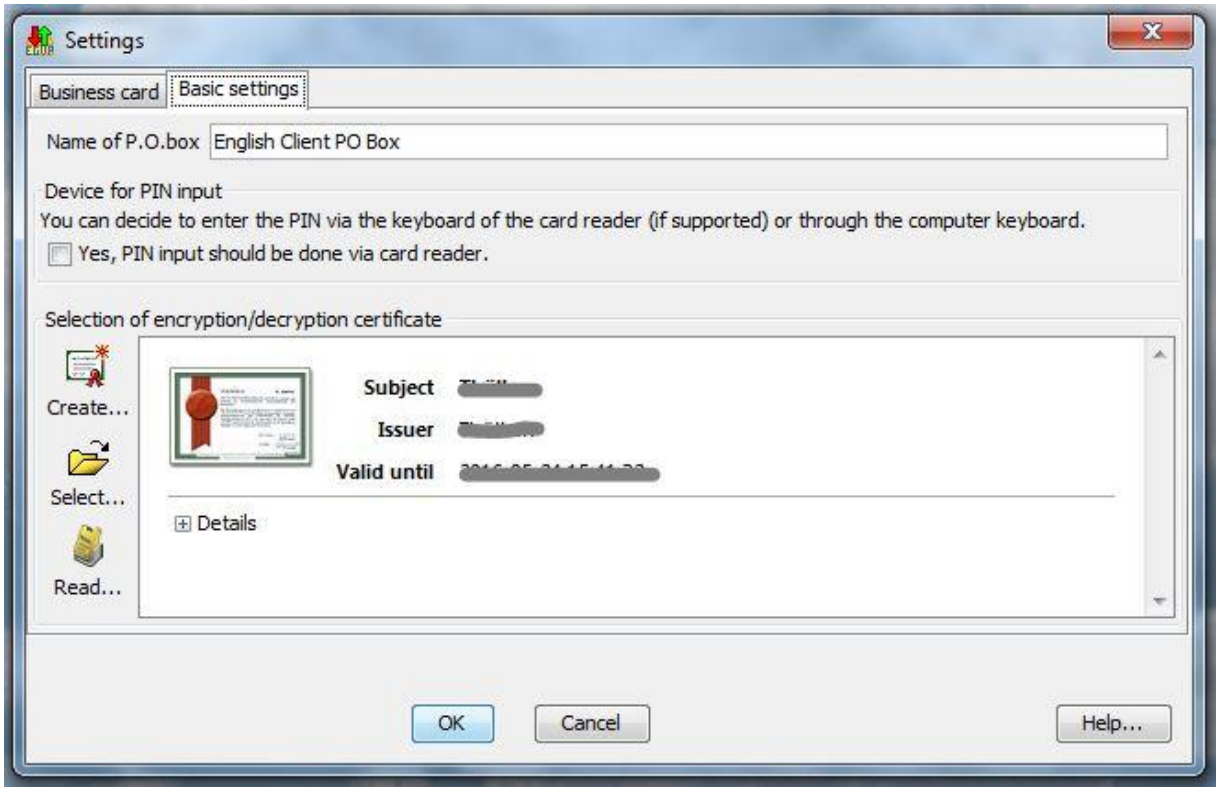

Figure 18: Certificate display

Mind that you have to have an active Internet connection before clicking OK because the business card data is transmitted to the directory service. This can take some time. Do not interrupt the process. Now your P.O.box is established and you can use the EGVP to send and receive messages.

6.1.1.3.1.2 Use of an existing software certificate

To select a software certificate click on "Select" and a new dialog opens.

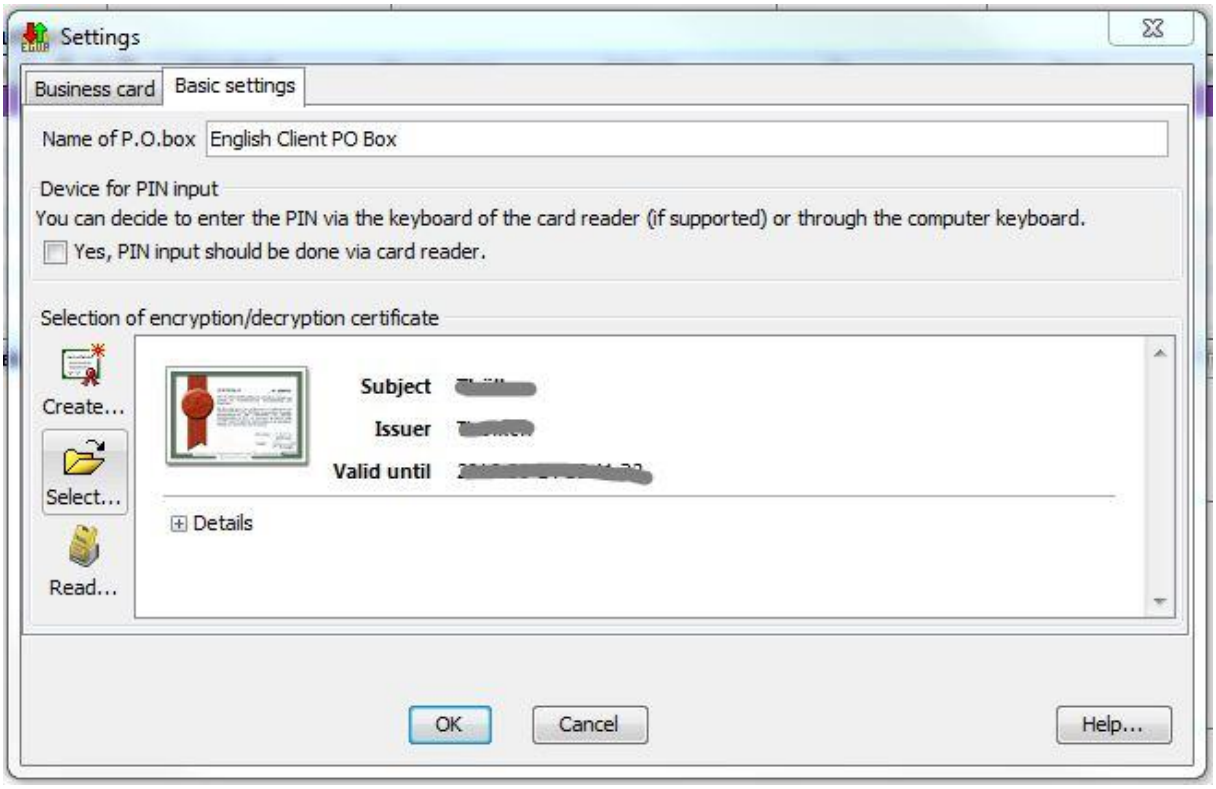

Figure 19: Software certificate selection

Choose an existing certificate and confirm with "Select".

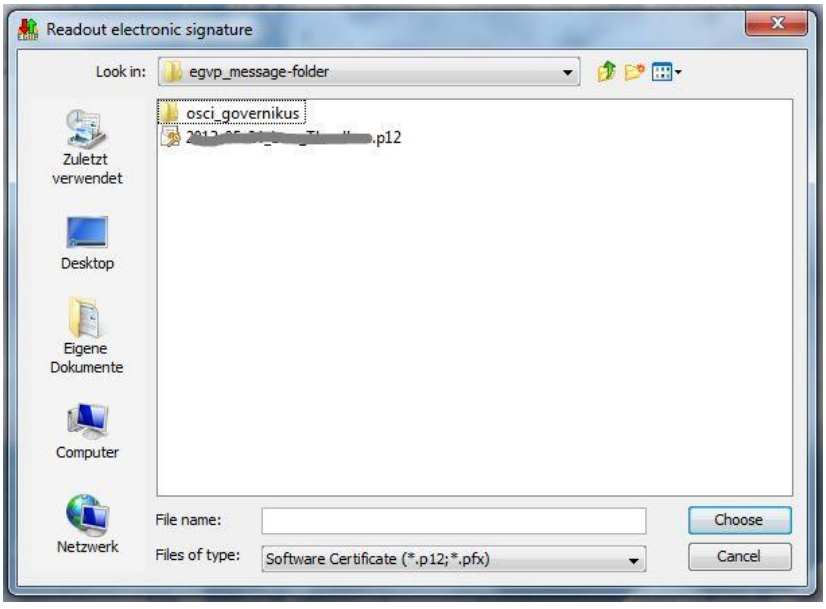

Figure 20: Certificate selection dialog

You are prompted for the PIN of the selected certificate.

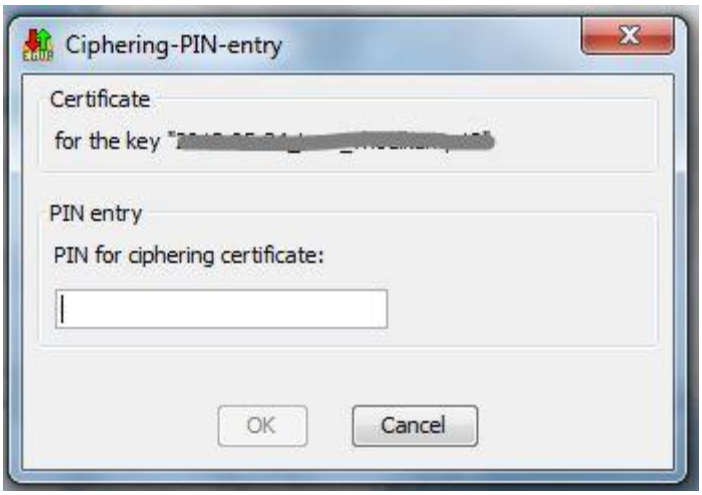

Figure 21: PIN entry

Finally the certificate is shown in the tab "Basic settings".

Confirm with "OK". Please mind that you have to have an active Internet connection before clicking the button because the business card data is transmitted to the directory service. This can take some time. Do not interrupt the process. Now your P.O.box is established and you can use the EGVP to send and receive messages.

6.1.1.3.1.3 Use of an existing smartcard

A card reader, connected to your computer and a smartcard are required to readout the certificate from the smartcard. To use the smartcard's certificate please click the button "Read-out".

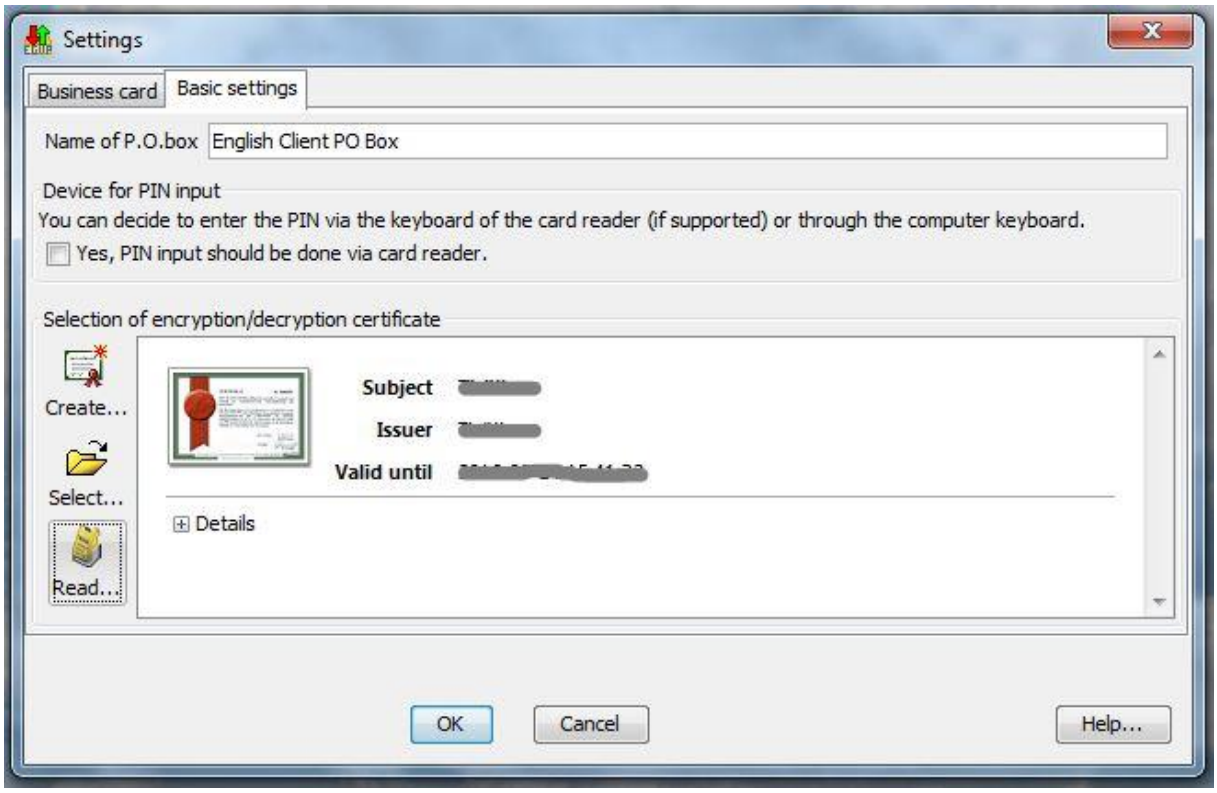

Figure 22: Certificate read-out

A window is displayed informing you about certain risks and limitations and you have to confirm this explicitly.

Question
Attention
You are about to use a cipher certificate from a smartcard for your P.O.box. It is recommended to use a software certificate. Nevertheless if you would like to use a hardware certificate, please consider the following restrictions in usability and functionality:
It is not possible to make a backup copy from a hardware certificate. This means if the card is damaged or lost, it is not possible to access your P.O.box anymore.
If using a hardware certificate in connection with only one smart card reader, a multiple signature with several signature cards is not possible.
Depending on the card type, it is possible that you have to enter a pin several times for every sending- and receipt procedure.
Do you really want to use a hardware certificate?
Yes
No
Help...

Figure 23: Notification when using a smartcard for establishing a post box

Afterwards the certificate is shown and you have to enter the corresponding PIN. Confirm the entry with "OK".

	Note: If you use a smartcard certificate to encrypt your P.O.box you have to enter your PIN with your smartcard reader repeatedly for every action (sending, receiving, user search)

Afterwards your certificate data is shown in the tab "Basic setting".

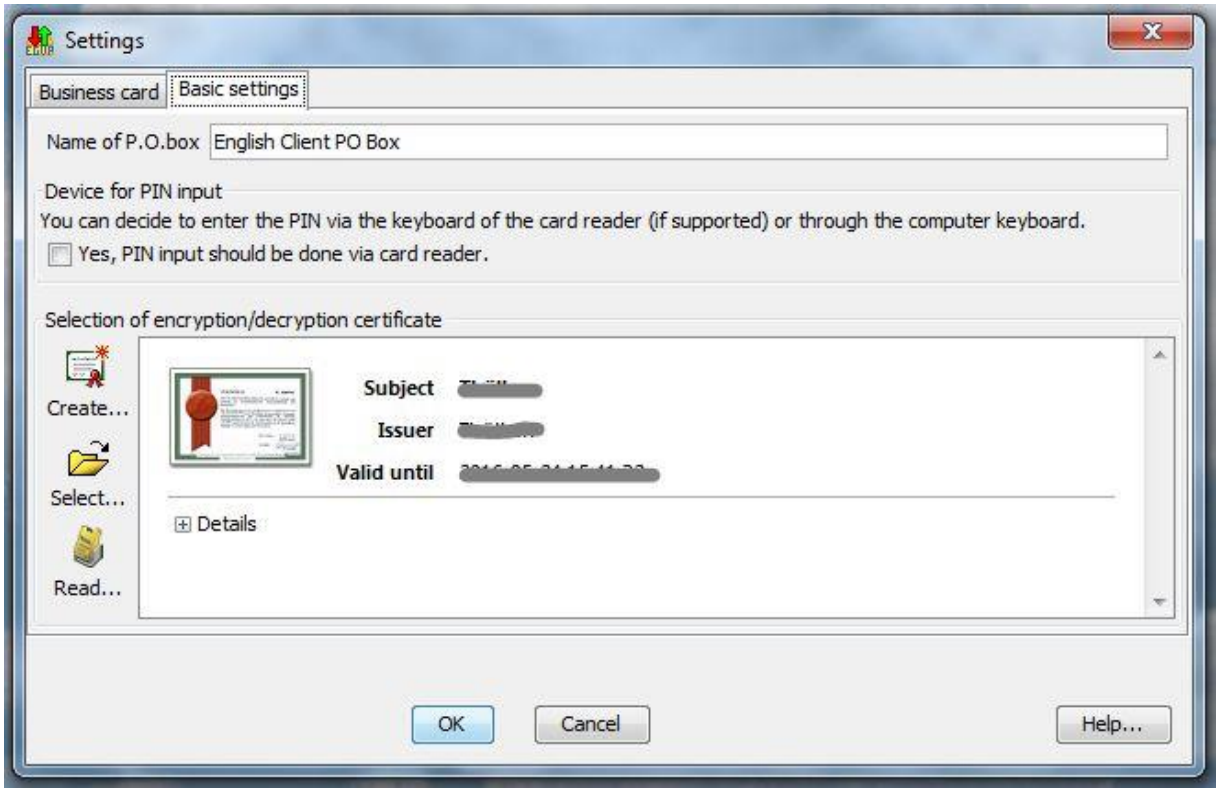

Figure 24: Certificate display

Confirm with "OK". Please mind that you have to have an active Internet connection before clicking the button because the business card data is transmitted to the directory service. This can take some time. Do not interrupt the process. Now your P.O.box is established and you can use the EGVP to send and receive messages.

	Note: Note that locked certificates cannot be used to establish a P.O.box.

Note:

Note that with the beginning of EGVP version 2.6.0.0 and S.A.F.E. there are special requirements of using the smartcard certificates.

The used smartcards have to contain a cryptographic key which enables deciphering and designating. This means that the functions to cipher and to decipher (KeyUsage "keyEncipherment" and "dataEncipherment") as well as to authenticate (KeyUsage "Digital Signature") have to be provided by one certificate.

In case these functions are provided with separate certificates, they won't fulfil the requirements of the registration service S.A.F.E..

6.1.1.3.1.4 Exchanging the P.O.box certificate

In case you want to exchange an already embedded certificate, e. g. because it will soon expire, you can do this in the basic settings as well. Further details are described in chapter 6.2.4. After confirming the selection of a new certificate with the OK button, the certificate is exchanged. Before exchanging the certificate, the application checks for new messages for the P.O.box. Exchanging the certificate can only be completed after all messages are retrieved.

Note:

Please note that messages, which were sent prior to exchanging the certificate, cannot be retrieved again after you have exchanged the certificate.

6.1.2 Open a P.O.box

After the first start of the application and after you have established a P.O.box, a log-in window is displayed. You can choose an existing P.O.box. Select a P.O.box from the listing and click OK. In case only one P.O.box was established the dialog "P.O.box selection" is not displayed but you will get the PIN-entry dialog directly. The PIN-entry-dialog appears and you can enter your PIN, which is assigned to the P.O.box.

After successfully entering the PIN the user interface is shown and you can create, send and receive messages. On opening the P.O.box the applications checks whether the integrated certificate is expired or not. Will it expire in less than 90 days, an according note is displayed. Will it expire in less than 30 days, you are notified on every opening of the P.O.box and are offered to generate a new certificate. After the expiration of the certificate, the P.O.box can only be used with limited functionality: messages can be received, but it is not possible to create or to send messages.

	Note: The user is informed about a new version of EGVP as soon as the EGVP is launched or in case the EGVP is already running when an Internet connection is established. Prior to downloading a new version the EGVP has to be closed and restarted with an active Internet connection.

6.1.3 Delete a P.O.box

If you want to delete a P.O.box you can do this from "P.O.box/Delete".

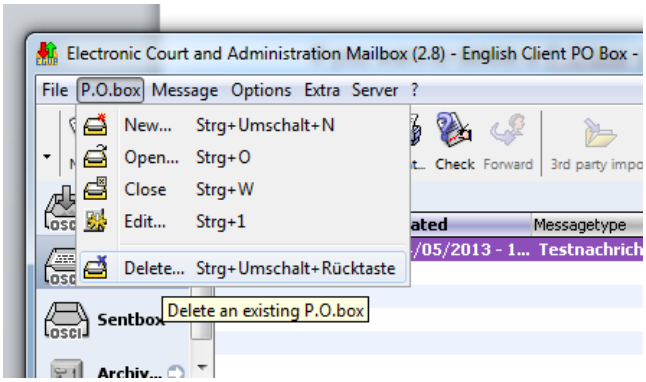

Figure 25: Delete a P.O.box

To delete a P.O.box you have to close it first (menu "P.O.box/Close"). The window "Select P.O.box" is displayed first. Choose the post box you want to delete and click "Delete". The button is only enabled on not active boxes. The post box will not be deleted until you have entered the correct PIN of the respective certificate. Before the P.O.box is deleted an automated query for not yet received messages is executed. If no messages exist on the OSCI Manager the P.O.box is deleted.

6.1.4 Close P.O.box

With selecting "Close" in the menu "P.O.box" you can close an already opened P.O.box. Now you can delete the P.O.box, open a new P.O.box, or close the application.

6.1.5 Edit P.O.box

Choose the "Edit" option in the P.O.box menu and the settings dialog for the active post box is displayed. You can change all specific parameters, e. g. your personal data (business card) or the name of the box and the assigned certificate. You can define another way of entering the PIN for the supported card readers as well.

	Note: If you use a smartcard certificate to encrypt your P.O.box you have to enter your PIN with your smartcard reader repeatedly for every action (sending, receiving, user search)

6.2 Use of the P.O.box

To use the P.O.box effectively there are several functions. These are briefly described in the following.

6.2.1 Settings

When selecting this option from "P.O.box/Edit" the settings dialog for the active P.O.box opens. All parameters for a P.O.box can be changed here. These are e. g. personal information of the sender (business card) as well as the certificate or P.O.box name. Users can also change the kind of PIN entry for supported card readers (PIN pad of the card reader or keyboard of the computer).

	Attention: Because identification data is only allowed to be saved on a smartcard it is mandatory to enter the PIN for a qualified signature on the PIN pad of the card reader only.

	Note: If you use a smartcard certificate to encrypt your P.O.box you have to enter your PIN with your smartcard reader repeatedly for every action (sending, receiving, user search)

6.2.2 E-mail notification

You can be informed when an OSCI message arrives in your P.O.box. To use this option you have to define an e-mail address. Choose the option "E-mail notification" under "options". The settings for the "E-mail notification" open.

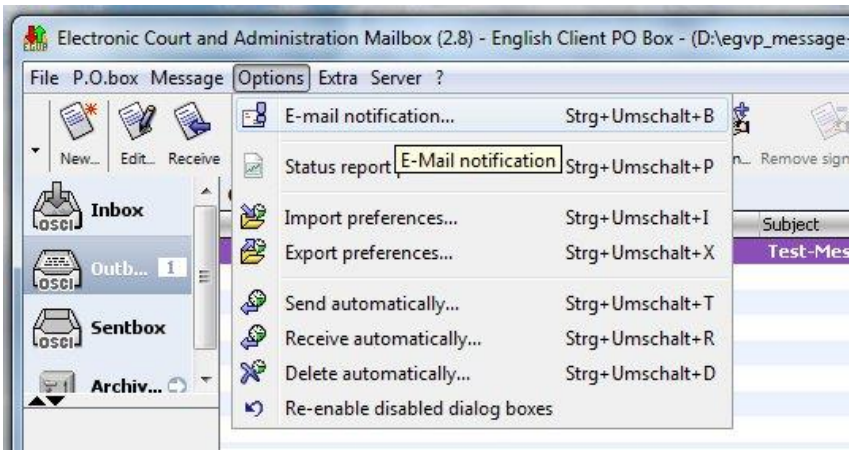

Figure 26: Menu "Options" e-mail notification

Enable the checkbox and enter your e-mail address in the input field. In case multiple addressees are to receive an e-mail notification a shared e-mail address has to be established before. Please confirm your entry with "OK".

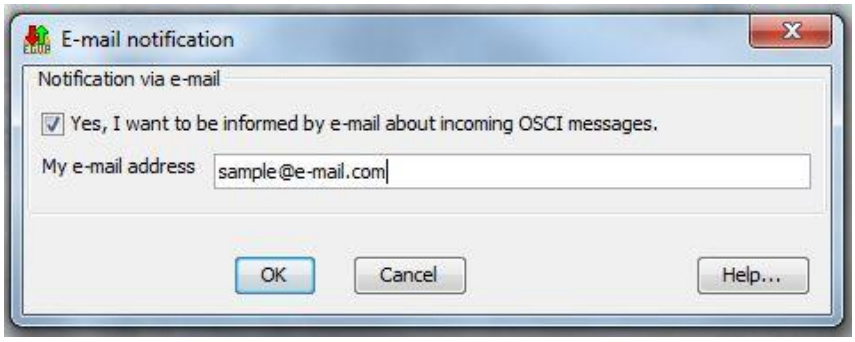

Figure 27: Settings for e-mail notification

Possibly the OSCI Manager has been set to send an additional e-mail notification if the addressee has not fetched the message within a defined period. This setting is subject to the operator of the OSCI Manager and has to be requested there.

6.2.3 Status report preferences

It is possible to report all incoming messages and their export. Additionally you can verify whether all messages stored in the OSCI Manager's P.O.box were received from the EGVP client.

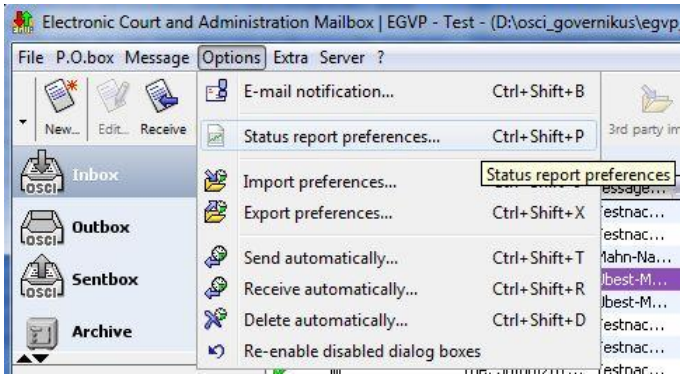

Figure 28: Menu "Options/Status report preferences"

Select the menu "Options/Status report preferences" to get the configuration dialog,

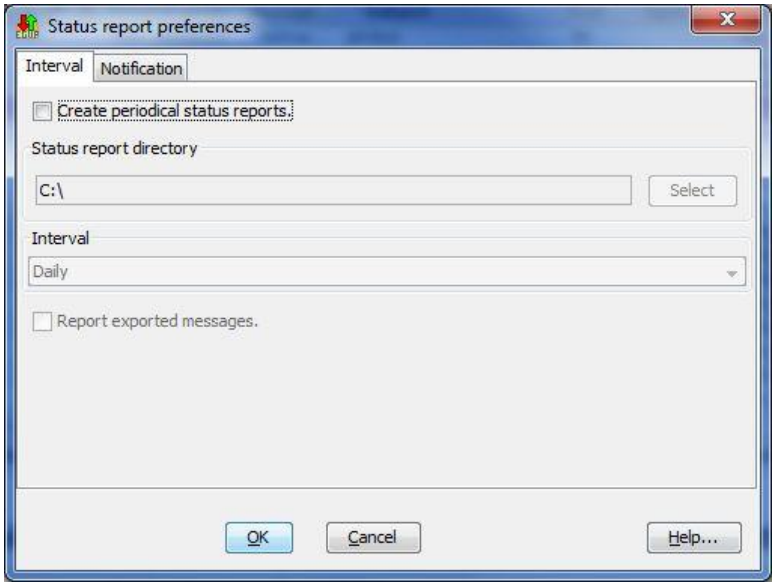

Figure 29: Tab Interval of "Status report preferences"

On the "Interval" tab you can define whether incoming and optionally exported messages are to be reported. Select a directory on your file system to store the reports. You have to make a decision of the interval of the report:

- Daily: Report from 00:00:00 o'clock of the current day to 00:00:00 o'clock of the following day.
- Weekly: Report from 00:00:00 o'clock on Monday of the current week to 00:00:00 o'clock on Monday of the following week.
- Monthly: Report from 00:00:00 o'clock of the first day of the current month to 00:00:00 o'clock of the first day of the following month.

For the first interval the settings apply restricted because information first is logged from the point of activation. Therefore the first interval will be from the point of activation of the report to the end of the edge which is elucidated above.

Is EGVP not available, the report will log again from the point of re-start EGVP. The file of the protocol first will be compiled if you try to receive or export messages after the expiry of the period of protocolling.

The report will be stored as .csv file, named with the P.O.box name plus the time of reporting (e. g. Example_post_box_26.08.2011-27.08.2011.csv). Every row of the .csv file contains the following information:

- Date/Time
- Action: receiving, export
- Message-ID
- Arrival at server
- Successful: yes/no

The verification that determines whether all messages from the OSCI Manager were received by the EGVP client, is executed when creating the report for the respective time. In case messages are not yet received, an additional verification report - as well in .csv format - is created in the same directory. This report contains the following information about the missing messages:

- Message-ID
- Arrival at server

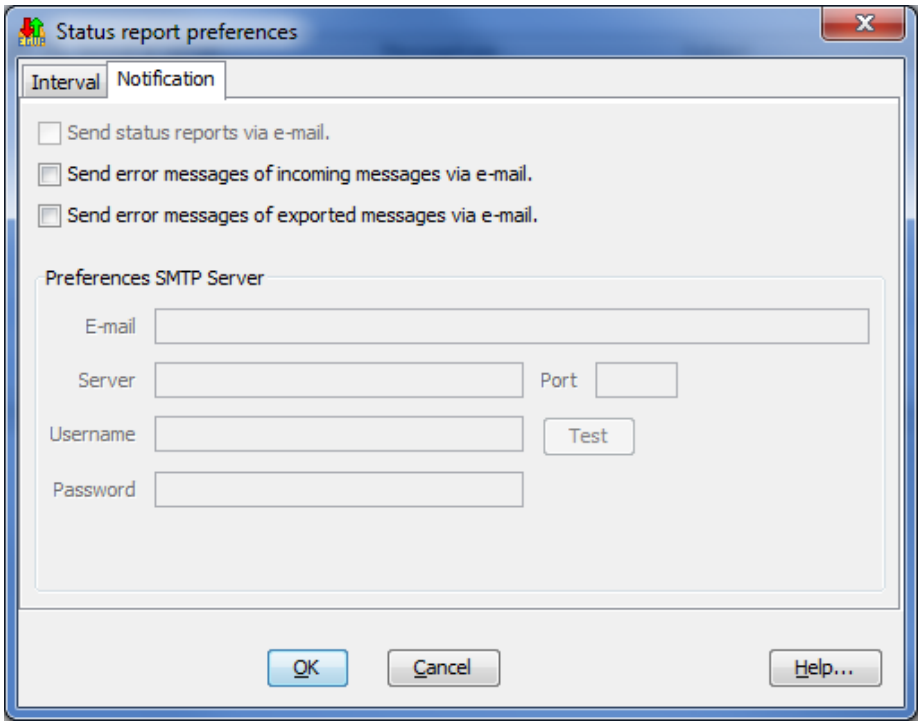

Figure 30: Tab Notification of "Status report preferences"

On the "Notification" tab you can decide whether or not the report is mailed to the defined e-mail account. After checking the respective box you have to configure the SMTP settings. Also define SMTP settings, if you want to receive possibly error information of incoming or

exported messages via e-mail. Click "Test" to send an email to check if the configured SMTP settings are all right.

6.2.4 Create new certificate

Selecting this option from the menu "Extra/create certificate" opens the window for the creation of a new software certificate.

	Note: The certificate is a self-signed certificate. It is only applicable for a basic signature (like e. g. the own name under an e-mail) and shall not be used for digital signing.

6.2.5 Changing the P.O.box certificate

In case you want to change the certificate for a P.O.box because e .g. it expires, you can do this from the menu "P.O.box/edit".

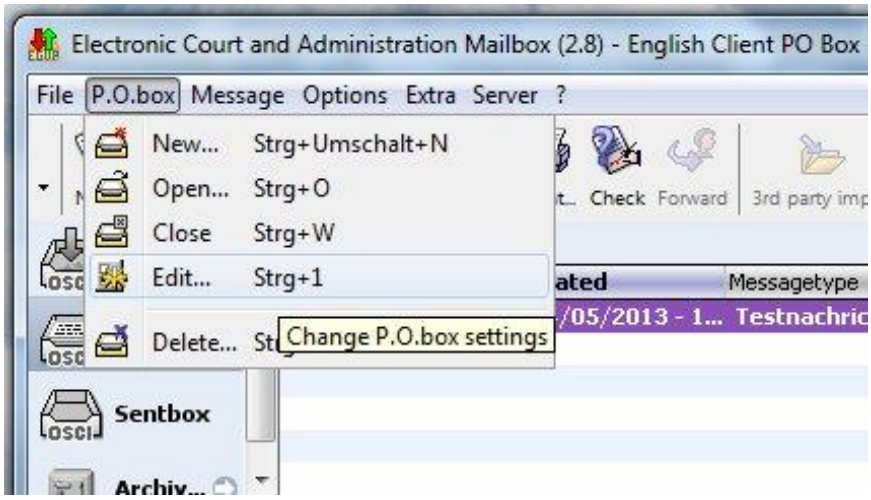

Figure 31: Exchange certificate

The "Settings" window opens. Go to the tab "Basic settings", select the certificate in question or create a new one and confirm with "OK". Before the certificate is changed the OSCI Manager is checked for messages for the P.O.box with the old certificate.

	Note: Old messages cannot be received again after you have changed the certificate.

Note:

With the expiration date the P.O.box cannot be used anymore and changing the certificate is no longer possible. Messages, which arrived before the certificate has expired, can still be fetched.

Please delete your P.O.box with expired certificates by your operator. You are allowed to request the user support for those purposes.

6.2.6 Import preferences 3rd party

With providing the generic import interface for business data the EGVP offers an interface for suppliers of custom software to pass content data including attachments. The EGVP imports this data and converts it to OSCI messages, showing these in the outbox.

Before first use of the 3rd party data-interface some settings have to be made. The menu item "Import preferences" displays the adjustment window for the import. Set the exchange folder for the provided custom data. Three subfolders, "Messages", where the EGVP will look after data to import, "DefectiveMessages" for messages that cannot be imported, and "SentMessages" to store the confirmation receipts, will be created automatically.

- "Messages": The custom software has to provide the data in subfolders for each message in this folder.
- "DefectiveMessages": Messages, which could not be imported correctly, are stored in this folder. The log.txt and the corresponding error message provide information about the failure cause.
- "SentMessages": Acknowledgements for sent custom software messages are stored here.

An automated import in a certain interval is possible. To activate it please enable the checkbox "Yes, import messages automatically from the import directory". You have to define whether an error message is shown on the screen or a record in the log.txt is sufficient.

The interface for suppliers of custom software is described in the document "Import interface for business data in EGVP". This document is provided by Governikus KG.

6.2.7 Import without exchange folder ("dynamic data transfer")

The dynamic data transfer offers transferring content data and attachments without defining an exchange folder (Options/import preferences/3rd party data transfer). Thus, you do not need to set up the 3rd party interface within the EGVP. Please ask your business software supplier, what kind of interface is needed

6.2.8 Export preferences

When choosing this menu option the dialog "Export preferences" with the three tabs "Inbox", "Sentbox" and "Archive" are displayed.

6.2.8.1 Inbox and sent messages

You can define whether messages are to be saved automatically into the folders defined here. A checkbox offers the option to delete the successfully exported messages directly from the inbox or sentbox.

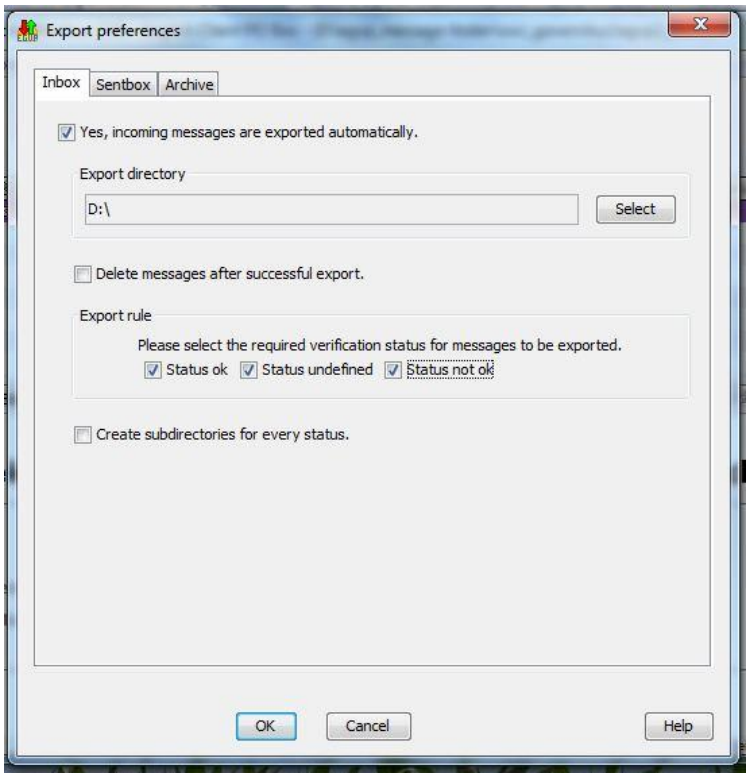

Figure 32: Export settings, "inbox" tab

Additionally you can define export rules for received messages. The rule applies on the status determined in the inspection sheet. Furthermore you can define that messages are stored in subfolders according to their status. In case you want to import the messages with another Communicator based application you should keep the checkbox disabled.

	Note: If you import exported messages from other P.O.boxes of EGVP, these messages must be exported in the main folder and not in subfolders. It is only possible to import data of other P.O.boxes from one directory.

The function will not be activated, if there is no rule and folder defined for received messages.

6.2.8.2 Archive

In the tab "Archive" it is possible to select the functions "Export archived messages" and "Delete archived messages". The settings can be taken separated by received and sent messages.

Export archived messages

The export function for archived messages is more likely a moving into an archive data backup. For that reason you can differentiate between received and sent messages when defining the minimum age (days) of messages to move. E. g. you can configure to move received archived messages into the backup folder after 30 days.

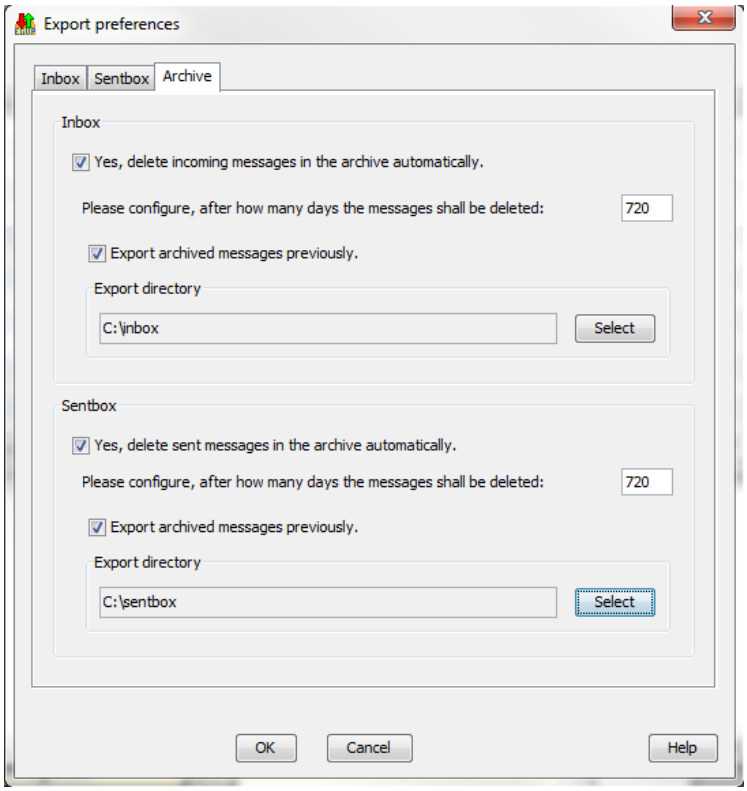

Figure 33: Export archived messages

By deleting messages after copying those to a defined folder the export will be initiated.

Delete archived messages

If you would like to delete messages exclusively, you only have to activate this function and to type in after how many days the messages shall be deleted.

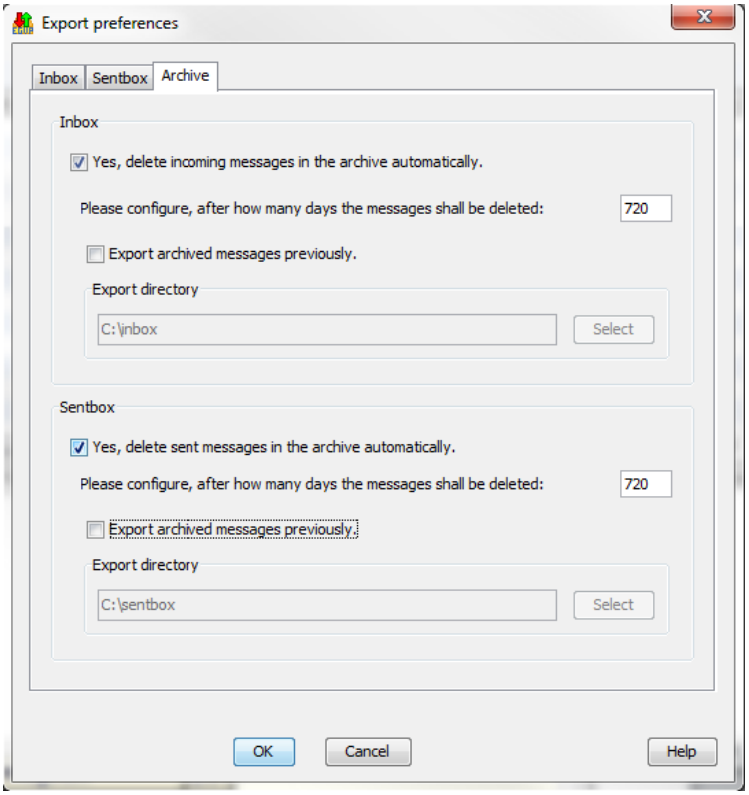

Figure 34: Delete archived messages

	Note: Sent messages are only archived from EGVP version 2.4 and higher. Messages that were sent with an earlier version of the EGVP will not be available in the archive.

	Attention: All settings in the tab "archive" only affect the messages in the archive. Messages, which exist in the "inbox" and "sentbox" as well are not affected.

	Note: You can define a period after which the messages will be automatically moved to an external directory. These settings have to be made separately for received and sent messages. Mind that messages which have been sent and received will be moved corresponding to the first rule for the archive.

6.2.9 Send automatically

Ready to send messages in the outbox, that must not be or are already signed, can automatically be sent. Configure the function in the respective dialog by defining an interval

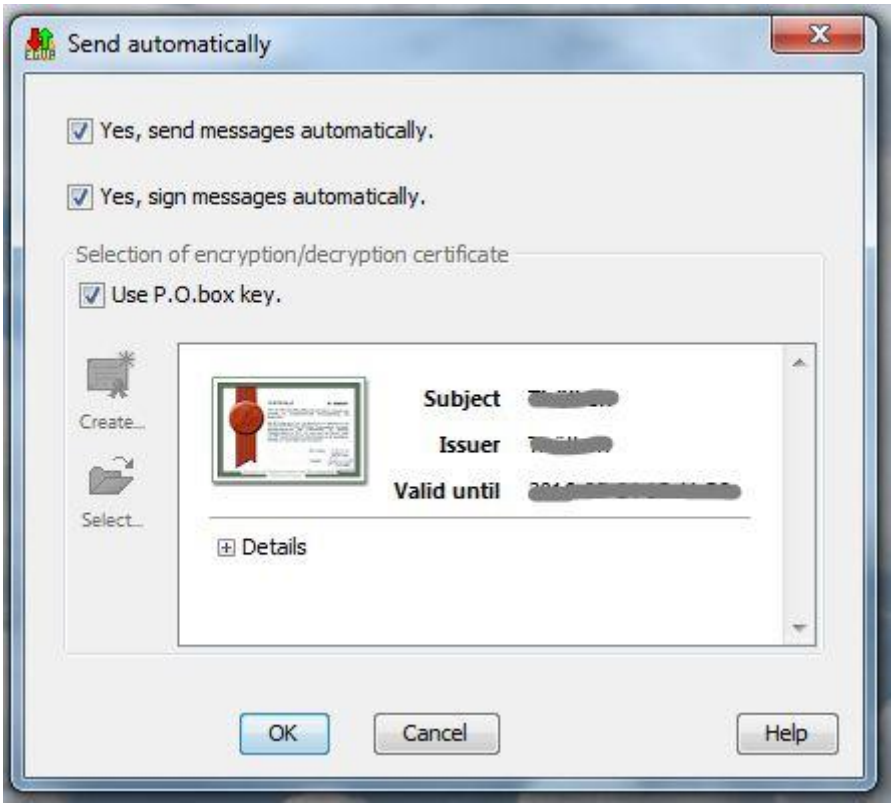

Figure 35: Settings for automatic sending

Additionally it is possible to configure the client to automatically sign messages with the advanced signature level. This feature needs the definition of the respective signature certificate to use for signing the message. You can use the P.O.box encryption and decryption certificate by clicking the checkbox, or by selecting a separate signature certificate. The respective PIN will be cached and encrypted locally, so you won't be asked for the PIN in future.

	Note: It is not possible to use PIN caching for qualified signatures, because it is not allowed to cache a PIN of smartcards.

In case a message cannot be sent it remains in the outbox and is marked red. If it was a temporary connection problem a new attempt to send the message is made. It is still possible to send messages by using the "Send all" or "Send selected" functions.

6.2.10 Receive automatically

Choosing this option will display the window "Receive automatically". Define the interval in minutes, how often EGVP has to check the OSCI Manager for messages and fetch them up automatically. The interval has to be at least 15 minutes.

	Note: The function "Receive automatically" is activated by creating a P.O.box and the setting of receiving messages amounts 30 minutes.

6.2.11 Delete automatically

Clicking this option displays the window "Delete automatically". This dialog offers you to automatically delete the locally stored messages from inbox and/or sentbox after a defined number of days.

The messages and their attachments however will stay in the archive. You can't define a period less than one day. Additionally you can define that only messages, which have already been exported, are deleted.

6.2.12 Address book

Here you will find all persons and institutions listed, to whom messaging with EGVP is possible. You have the possibility to choose between the tabs "users" and "favourites".

- In the "**users**" tab on the upper part of the window you can enter several criteria concerning the respective addressee. The results of the search are shown in the browser below. You can select more than one addressee at once by using the control key combined with the mouse. With the help of the arrow buttons you can skip between the address book pages. Narrow down the result by entering more search criteria.

- The "**favourites**" tab offers an overview of your preferred users. Therefore you have to mark these on the corresponding tab and add them with the button "add to favourites". You can also confine the selection with selection criteria and navigate through the pages with the arrow buttons.

A detailed description of this function is available in the chapter "Address book".

6.2.13 Subsequent certificate verification

The tab "certificates" in the lower part of the user interface shows all certificates belonging to a message. From the context menu each certificate can be subsequently checked online concerning their status (validity) via the verification server (OCSP/CRL-Relay) of the corresponding OSCI Manager. Please mind that you have to be online. The result is shown and can be printed or saved. A subsequent change of the results in the inspection sheet does not take place. For the validation a time has to be defined. By default this is the time of entry on the server (inbox and sentbox) or the time the message was created (outbox).

6.3 Information regarding the P.O.box

Information regarding the P.O.box is available from the menus "Server" and "?".

6.3.1 Menu Server

OSCI Manager

Selecting this option presents further information about the OSCI Manager for the application:

- **URL**: Displays the OSCI Manager's Internet address.
- **CA certificate**: Shows the CA certificate of the OSCI Manager’s public key.

In the lower right corner of the user interface the status of the LAST access to the OSCI Manager is shown. A red cross means that the last access failed, a green check mark indicates that the last access was successful. A grey question mark represents an unidentified status of the server.

Directory service

Selecting this option presents information about the directory service of the application:

- **User ID**: Shows the unique ID registered to the active P.O.box for the directory service.
- **Filter ID**: Shows the key needed for the general address filter. This means, that e. g. registered clients will only see recorded backends as available receivers in their address book, while backends can see all occupants.
- **URL**: Displays the directory service's Internet address.

Additionally the directory service's CA-certificate is shown. In the lower right corner of the user interface the status of the LAST access to the directory service is shown. A red cross means that the last access failed, a green check mark indicates that the last access was successful. A grey question mark represents an unidentified status of the server.

Verification server (OCSP/CRL-Relay)

This option shows the URL and certificate of the used verification server (OCSP/CRL-Relay). It is possible to select a verification server (OCSP/CRL-Relay) of a selective list. The certificate is necessary for the response, when certificates are validated online.

In the lower right corner of the user interface the status of the LAST access to the verification server (OCSP/CRL-Relay) is shown. A red cross means that the last access failed, a green check mark indicates that the last access was successful. A grey question mark represents an unidentified status of the server.

6.3.2 Menu "?"

Help

Selecting this option will show the help, find information of the current window or the entire application here.

About EGVP

This menu item shows the information about the application's version.

6.4 Create messages

Warning:

With the English EGVP client, messages must only be created via the import interface for 3rd party software and not via the message window for the time being.

Messages can be created with the message dialog or by using the 3rd party import (generic import interface). Both options are described below.

6.4.1 Create a message with the message dialog

To create messages click the "create messages" button in the user interface or choose "New" from the "Message" menu. The message window opens. In the message window messages can be created, signed if necessary and either be stored in the outbox or sent instantly.

After the selection of an addressee and all further entries, you can save the message in the outbox or send it right away. Optionally you can add attachments. You also have to decide on a message type and a signature level (qualified, advanced, or unsigned). To select a signature level, choose the according entry from the dropdown list.

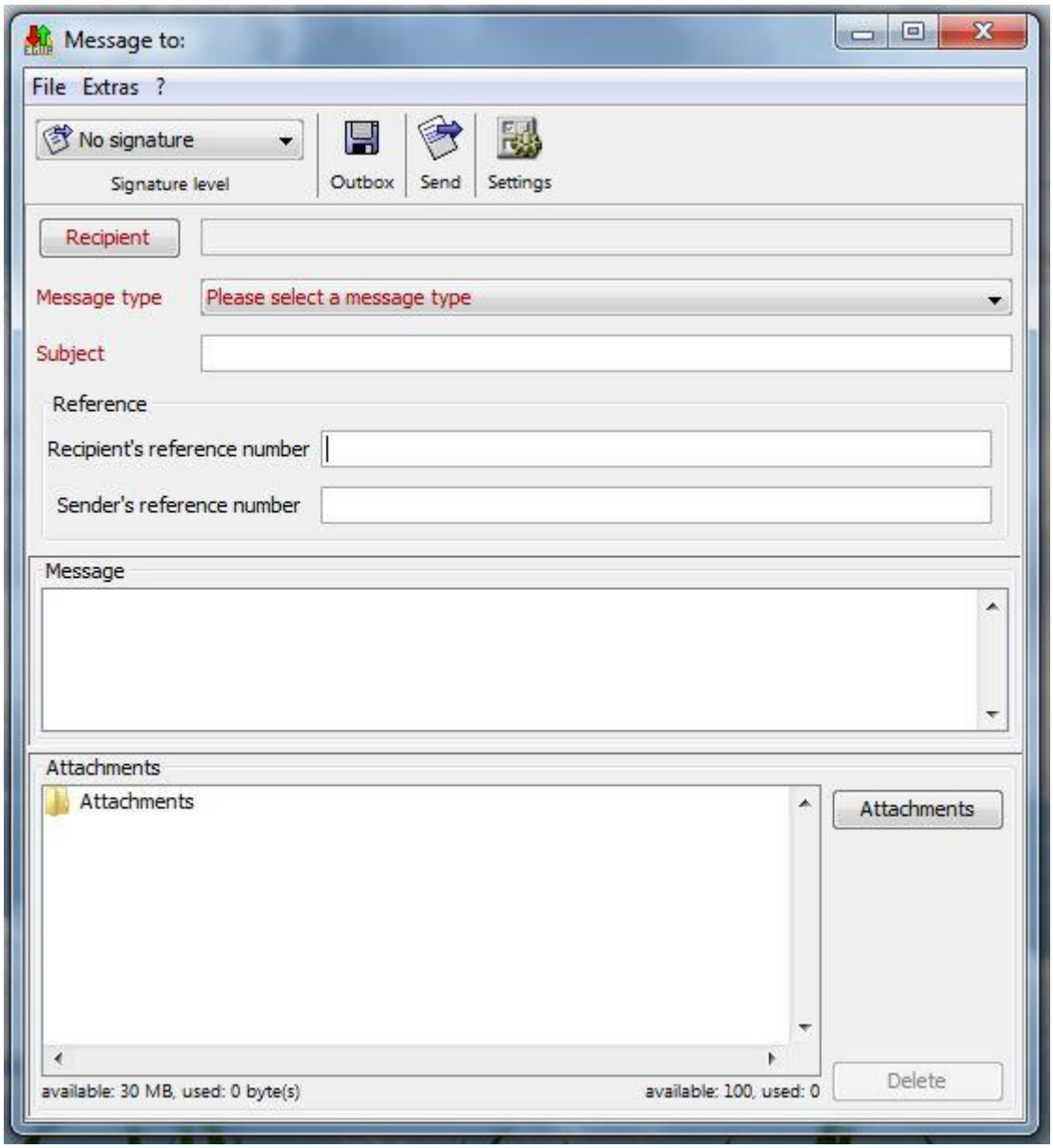

Figure 36: Message window

Menu File

Here you can define the signature level and save it to the outbox. You can also cancel the creation of the message by clicking "Quit".

Menu Extras

Select "Settings" to open the settings for the message dialog. You can define a default message type with default values for every message dialog in the tab "General". You can also define a default directory for attachments. In the tab "Instant sending" settings for sending messages without caching in the outbox can be defined.

Menu "?"

The help for the message window can be opened here.

Addressee

Click on "select" for the address book. The entry of an addressee is mandatory. The necessary steps for selecting an addressee are described in chapter 6.5 in detail.

Message type

Each message must have a defined message type. With the message type, a certain distribution rule may apply within the addressee's organisation. It is the sender's task to define a certain type to make sure that the message can be handled correctly. The listing below shows further information for the assignment of message types:

Name of the message type	meaning of the message type
Allgemeine Nachricht	general message
HR-Beteiligter	commercial register message
Mahn-Antrag	"ProfiMahn" application data of an applicant or process procurator to the dunning court (incl. online dunning application, "OptiMahn" etc.)
Testnachricht	filing of test messages

(As of June 2014)

Subject

In this mandatory field you have to enter the subject of your message. The addressee can see this text first, when the message is displayed in his P.O.box.

Reference

In this field the reference for the message can be selected. You can select between "no reference" or "addressee's reference". Additionally the sender's reference can be used.

Attachments

Button "Attachment":

This opens the file explorer and you can select attachments for your message. Courts and administration only accept file formats, which were approved. The corresponding acceptance regulation can be found at the website of each court/administration or at http://www.egvp.de.

In case you add one or more files, whose format is not accepted, according information is displayed. This also applies when changing the recipient. Nevertheless, you can attach this file to the message. This way, exhibits can be attached, whose file format are not approved.

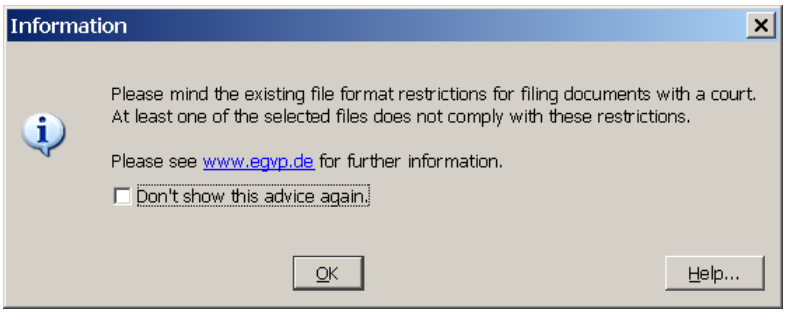
Information
Please mind the existing file format restrictions for filing documents with a court.
At least one of the selected files does not comply with these restrictions.
Please see www.egvp.de for further information.
Don't show this advice again.
OK
Help...

Figure 37: Notification when trying to add a file with a non-accepted extension

From the file header a check is initiated to ensure that the file suffix is consistent with the expected file format. If there is no consistency a respective note is shown.

Button "Delete":

If you want to remove files from the message, select these in the window and click "delete" afterwards.

	Note: Do not use files with the same name as the content data as attachment. Usually content data is named: "herstellerinformation.xml", "nachricht.xml", "nachricht.xsl", "visitenkarte.xml", and "visitenkarte.xsl".

	Note: If you intend to send a message of XJustiz, please attach the according file using the identifier "xjustiz_nachricht.xml". This way the message conforms to the OSCI transport profile for XJustiz.

6.4.1.1 Storing the message in the outbox

With a click on the button "outbox" the complete message is saved in the outbox. The message dialog closes. If you opted for storing the message in the outbox before sending, you can make sure that the message was saved correctly by clicking on the "outbox" in the P.O.box bar and selecting the message from the listing. All data is shown in the tabs in the lower part of the user interface.

6.4.1.2 Instant sending

By clicking the "Send" button, the message is sent. If necessary, it has to be signed beforehand. If you opted for instant sending, the message is stored in the sentbox. You can view the message by clicking on the "sentbox" in the P.O.box bar and selecting the message from the listing. All data is shown in the tabs in the lower part of the user interface.

Under "Settings" in the tab "Instant sending" you can define additional pre-adjustments.

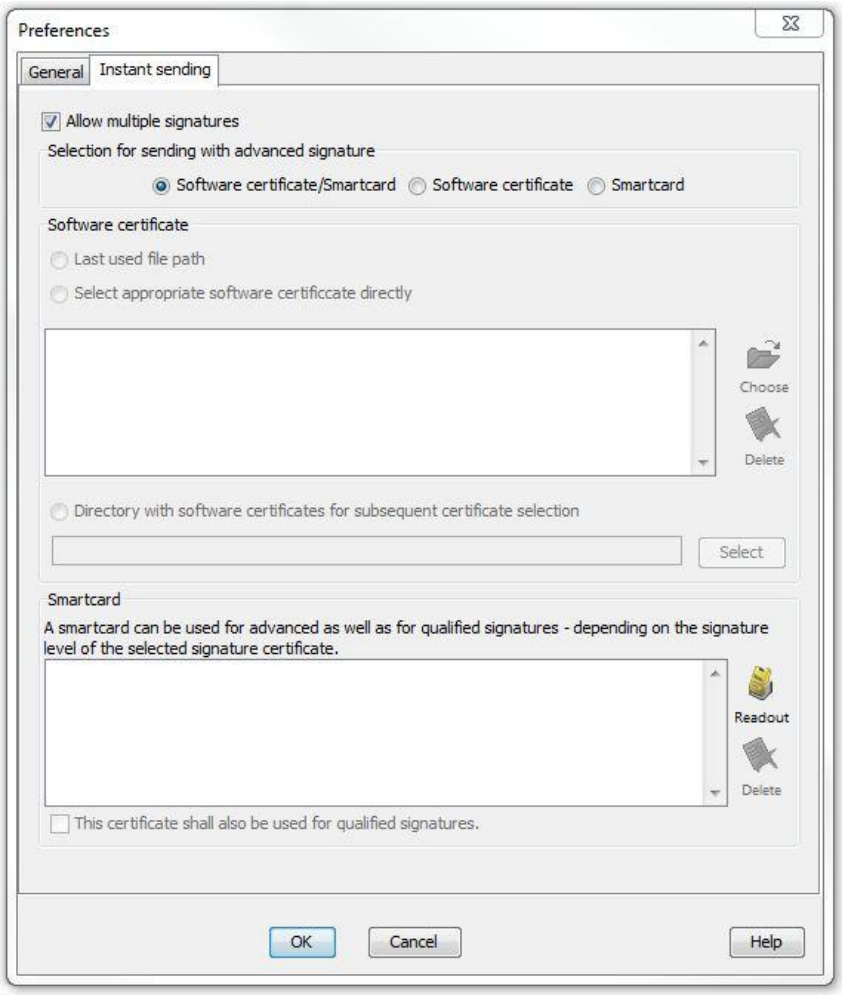

Figure 38: Settings "Instant sending"

You can define whether you want to allow multiple signatures to be applied to a message. The according checkbox is activated by default. On sending a message by clicking the "Send" button in the message dialog, you are asked if you want to apply more signatures. If you respond "yes", the dialog for selecting the signature certificate is shown again. You can apply signatures as long as the according question is answered with "no". If you always want to apply only one signature, deactivate this checkbox.

Selection for sending with advanced signature

Decide, whether you want to sign messages with signature level "advanced" with a software certificate or with a smartcard. The option "Software certificate/Smartcard" declares that you do not want to make a selection now and that you decide directly by signing the message.

	Note: Settings for advanced signatures are also used for signing messages from the outbox.

Software certificate

If you want to use a software certificate to sign messages with the signature level "advanced", you can define here, where the certificate to be used is stored. The last used

file-path is used by default. In case the settings haven't been changed, the user directory is selected. Alternatively, you can directly select the appropriate certificate. You can also define a directory, wherein several possible certificates are stored.

If a file-path/directory is selected, you can select the appropriate certificate before transmission of the message. After entering the PIN the message is sent.

Smartcard

A smartcard can contain advanced as well as qualified signature certificates. Therefore, an according selection can be made in this section. If a message has the signature level "advanced" and is to be signed with a signature certificate stored on a smartcard, this certificate can be lodged here. In case a qualified certificate is available on the smartcard and is to be used for signing messages, the according checkbox has to be activated. After entering the PIN the message is sent.

6.4.2 Create a message using the 3rd party import (generic import interface)

Instead of using the message dialog to create a new message, it is also possible to generate a note with business software and import it into the EGVP (dynamic data transfer). Using the interface to create the message, editing with the message dialog is no longer necessary. An imported message cannot be changed. After successful import the message is in the outbox. If necessary it can be signed here before sending. Please ask your business software supplier about the required interface.

6.5 Address book

In the following the address book and the possibility to select addressees is described in detail.

6.5.1 Select message addressee using the address book

The dialog "Select message addressee" shows all possible receivers, stored in the directory service. Here all persons and institutions are listed to whom messaging with EGVP is possible. This window is displayed after clicking the "Addressee" or "To" button in the message dialog or choosing "Address book" from the "Extra" menu.

As soon as you click on the button "To” or "Addressee” or open the option "Address book” in the "Extra” menu from the application window, a window showing three tabs opens. You can choose one or more addressees from one of them. The tab displayed in the foreground is the one you last opened.

	Note: The overviews in the address book can be sorted in ascending or descending order by columns. The column, which is currently active, is highlighted by colour and marked by a prefix ▼ for descending and a prefix ▲ for ascending order. Click on a column to switch from a descending to ascending order or reverse. Click on a different column to make this one the active for sorting

6.5.2 Tab "Users"

On the first displayed tab of the address book it is possible to choose one or several addressees. Therefore you can confine the selection of displayed receivers with the input fields in the upper part of the window. To start searching, press "Enter". The results of the search are shown in the browser below. Results can only be displayed when the number of hits is less than 500. If the number of hits is greater, you are notified and advised to confine your search.

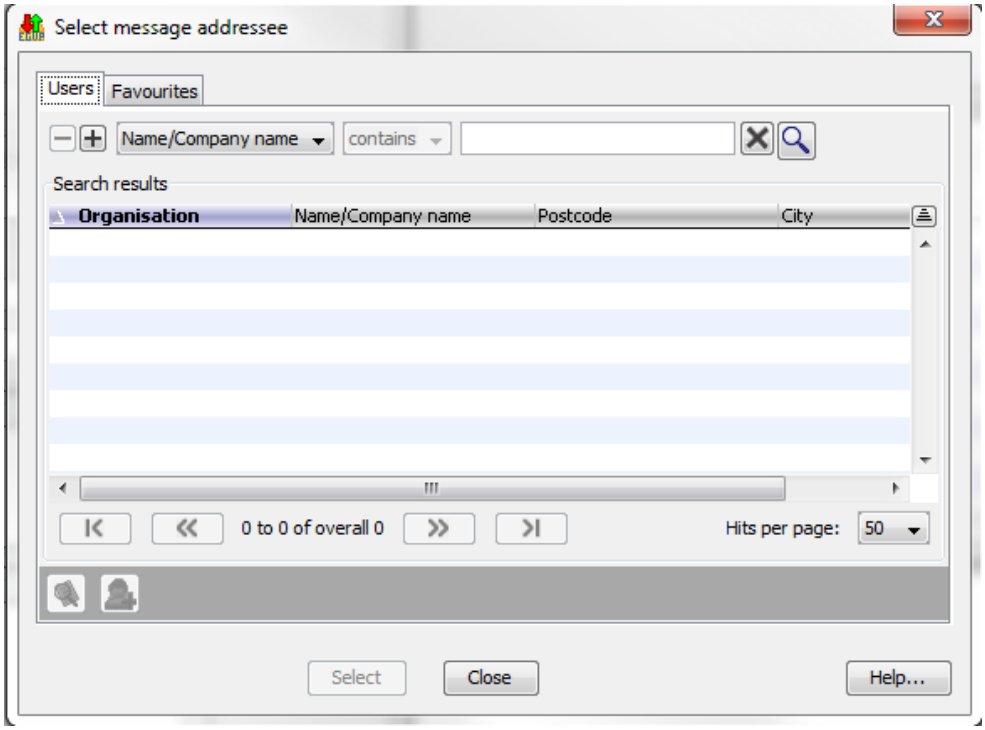

Figure 39: Address book - tab "Users" with example receivers

Following possibilities for working with the address book are available:

Input field "Search for entry"

Narrow down the results by entering several search criteria: With the drop down menu you can choose which search criteria you want to enter. If you want to enter more than one you can add a new row with the button prefixed+. You can remove a row from the search with the − button. To the right of the input field in the first row is the ✕ button. With this button you can reset all entries concerning your search. When you enter different search criteria the browser will only display a reduced selection based on your criteria.

Note:

For a logical AND combination of search criteria you have to add a new row and choose the same category as before. Entering space characters also leads to a logical AND combination.

Example:

Organisation "Obere Landesbehörde" in Nordrhein-Westfalen will only display results, which have "Obere" and "Landesbehörde" in the name and are located in Nordrhein-Westfalen.

Display "search results"

The columns "Organisation", "Name/Company Name", "Postcode", and "City" (default display) will give you an overview of all addressees fitting the search criteria. If you would like to see more columns, you have to add them from the context menu (click with the right button of the mouse on the topic of the column). It is as well possible to set the default values with the help of the context menu.

Click the column title to change the sorting up- or downwards within the respective column. Mark one or several entries with the mouse. For multiple selections use the mouse in combination with the shift- or control key.

Note:

It is required to select at least one column of the results, therefore it is not possible to remove all columns.

Navigation "Hits per page"

Define the maximum number of addressees to be shown on a page. You can choose between 50, 100, 250, or 500 addressees per sheet.

Navigation "(n1) to (n2) of overall (n3)"

These numbers shown in the information index indicate, which page is actually displayed and how many addresses fit the search criteria.

- (n1) is the number of the first displayed address on the actual shown page
- (n2) is the number of the last displayed address on the actual shown page
- (n3) is the number of all receivers of the current address book regarding the search criteria

E. g.: "51 to 100 of overall 434" with defined "50 hits per page" will give you the information, that you are positioned on the second page of 11 in this address book.

	Note: In case no entries matching your search are found no hits are displayed.

Navigation with the arrow buttons

In case the search criteria will display more addressees than defined in "hits per page", you can navigate between the several address book pages by using the arrow buttons. Click

- "|<" navigate to the first address book page
- "<<" go back one page
- ">>" go forward one page
- ">|" navigate to the last address book page

Button: Details

Marking an addressee in the result browser will enable the "Details" button. Click this button to see the information window containing the business card and all certificate information of the marked addressee.

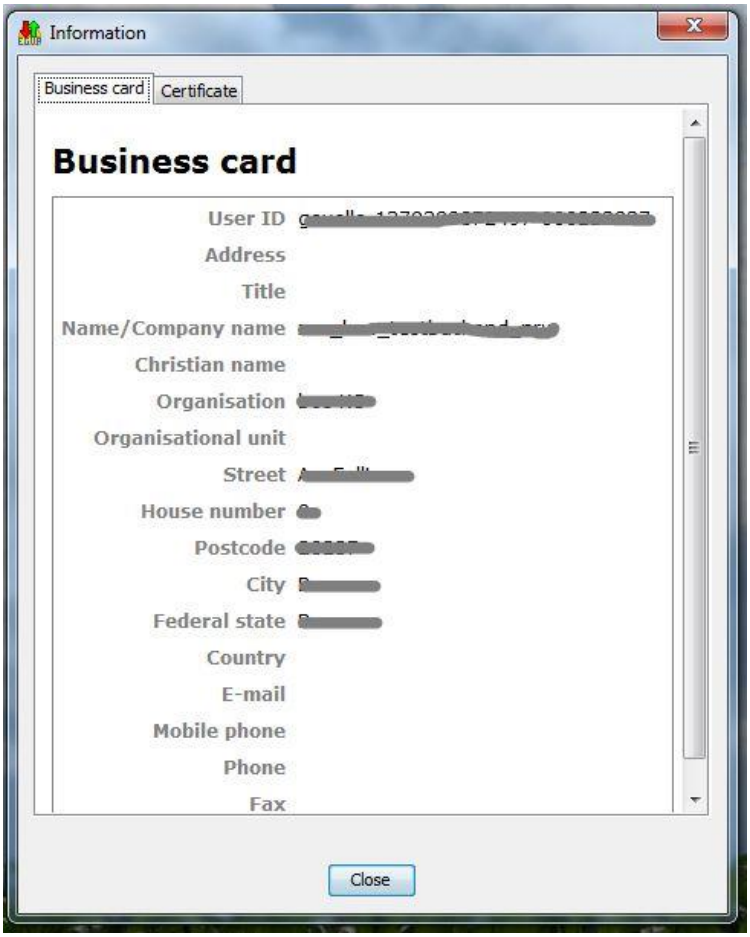

Figure 40: Details of the respective addressee

Button: Add to favourites

If you send messages to a specific user often it can be useful to add this user to your favourites. A click on the button will add the marked user to your personal favourites. When sending new messages to this user you can choose the user directly from your favourites. The number of favourites is limited to 100.

	Note: If you have your favourites well organised and up-to-date you only need the tab user to maintain your favourites. If you have selected an addressee once from the favourites EGVP will offer the favourites tab as first choice on the next start. The tab, which is displayed first is always the one, the last selection was made from.

Button: Select

This button is only displayed when opening the address book from the "Message" dialog. Mark the designated receiver and choose "Select" to store the addressee to the edited message. In case you have marked more than one addressee, all receivers will be placed into the message.

Button: Close

Closes the address book without choosing a receiver and change back to the "Message" dialog or the main application.

Button: Help

A click on the button will open the help for the address book.

6.5.3 Tab Favourites

It is possible to add often addressed users to your favourites using the respective button on that tab. If you have your favourites clearly arranged and up-to-date you have quick access to the designated recipient. Moreover, you can use favourites to create messages without existing internet connection, as in this case only favourites can be selected as recipients.

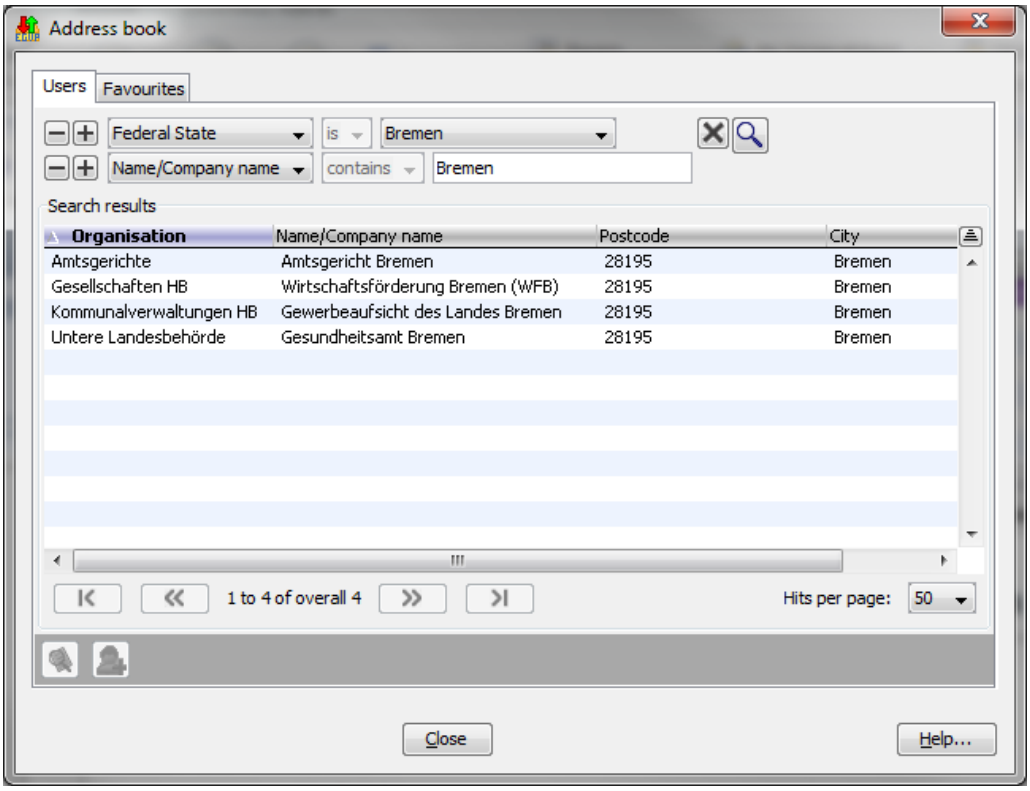

Figure 41: Selecting an addressee from the favourites tab

Input field "Search for addressee"

Narrow down the result by entering several search criteria: With the drop down menu you can select, which search criteria you want to enter. If you want to enter more than one you can add a new row with the button prefixed +. You can remove a row from the search with the minus button −. To the right of the input field in the first row is the reset button ✕. With this button you can reset all entries concerning your search. When you enter different search criteria the browser will only display a reduced selection based on your criteria.

	Note: For a logical AND combination between search criteria you have to add a new row and select the same category as before.

Display "Overview"

The columns "Organisation", "Name/Company Name", "Postcode", and "City" (default display) will give you an overview of all addressees fitting the search criteria. If you would like to see more columns, you have to add them from the context menu (click with the right button of the mouse on the topic of the column). It is as well possible to set the default values with the help of the context menu.

Click the column title to change the sorting up- or downwards within the respective column. Mark one or several entries with the mouse. For multiple selections use the mouse in combination with the shift- or control key.

	Note: Receivers are tagged in red if messages cannot be sent, because their software certificate is expired.

Navigation "Hits per page"

Define the maximum number of receivers to be displayed on a page. You can select between 50, 100, 250, or 500 addressees per sheet.

Navigation "(n1) to (n2) of overall (n3)"

These numbers shown in the information index indicate which page is actually displayed and how many addresses fit the search criteria.

- (n1) is the number of the first displayed address on the actual shown page
- (n2) is the number of the last displayed address on the actual shown page
- (n3) is the number of all receivers of the current address book regarding the search criteria

E. g.: "51 to 100 of overall 434" with defined "50 hits per page" will give you the information, that you are positioned on the second page of 11 in this favourites list.

	Note: In case no entries matching your search are found no hits are displayed.

Navigation with the arrow buttons

In case the search criteria will display more addressees than defined in "hits per page", you can navigate between the several favourites pages by using the arrow buttons. Click

- "|<" navigate to the first favourites page
- "<<" go back one page
- ">>" go on one page
- ">|" navigate to the last favourites page

Details button

Marking an addressee in the result browser will enable the "Details" button. Click this button to see the information window containing the business card and all certificate information of the marked receiver.

Remove from Favourites button "−"

To keep your favourites clearly arranged it is recommended to clean them up from time to time and to remove unused addressees. Mark the respective receiver and click on the "Remove from favourites" button.

Select button

This button is only displayed when opening the address book from the "Message" dialog. You can mark the designated receiver and use "Select" to store the addressee to the edited message. In case you have marked more than one addressee, all receivers will be placed into the message.

Close button

Click the close button to cancel the selection process and to return to the message window or to the user interface.

Help button

With this button you can open the help.

6.6 Working with messages

This scenario describes all functions, which are available from the menu "message". You will be able to create, edit, process, send, and receive messages.

6.6.1 Send messages

After a message was created and stored in the outbox it can be sent. In the following the two functions for sending will be described.

Note:

In case the transfer failed because the addressee was deleted in the meantime, an error message is shown.

Send all

When selecting this option all messages stored in the outbox and signed, at least as their previously defined signature level will recommend, are sent immediately. After sending, the messages, their transmission reports, and acknowledgement information is stored to the sentbox.

To use this feature it is necessary that there are messages stored in the outbox for sending and that an active Internet connection is available. The send status is displayed in the status section at the bottom of the P.O.box bar. You can see that message x of n is sent and there will be a life indicator to show the finishing progress status.

Send selected

When selecting this option all highlighted messages stored in the outbox and signed, at least as their previously defined signature level will recommend, are sent immediately without further notice. After sending, the messages, their transmission reports, and acknowledgement information are stored to the sentbox.

To use this feature it is necessary, that there are messages stored in the outbox to send and that an active Internet connection is available. The menu option has the same function as "send selected" from the tool bar.

Note:

In case more than one message was sent at the same time and some problems occur during sending, the respective not sent messages will be marked red in the outbox. The client will show only the last message after finishing the sending.

To see the particular note for a not sent message select the message and use the "send selected" function. The error message is displayed, if the problem still exists, otherwise the message is sent immediately

Note:

In case the Internet connection is interrupted while sending, it is possible that the receiver got the message, but it is still stored in the outbox instead of the sentbox. Contact the addressee to make sure, the message was received or send it again.

Note:

It is not possible to send messages to addressees with expired P.O.box certificates.

6.6.2 Receive messages

The "Messages" menu contains two functions for receiving messages. These features are also available with the function bar buttons:

Receive

When starting this function all messages related to the active P.O.box and waiting at the OSCI Manager will be collected and displayed in the inbox. Please note that an active Internet connection is required.

Fetching new messages is done without further notice. The status will be shown in the status section at the bottom of the P.O.box bar. You can see that message x of n is received and there will be a life indicator to show the finishing progress status.

In case no message is available for you the message "There are no messages for the selected P.O.box on the server" is shown. Otherwise the external messages are now displayed in the inbox. The menu option is the same as the one from the tool bar.

Note:

After a message is received it is displayed as incomplete if:

- the message format of the received message does not conform to the defined format (OSCI message not complete) or
- it wasn't possible to encrypt the message completely.

The message will be marked red in the inbox and the message status is undefined. The OSCI Manager will mark the message as "not yet collected". The message will neither be archived nor exported.

Try to receive the message again. Please contact the support, if the message is displayed again.

Attention:

A completely received and encrypted OSCI message can possibly not be visualised completely. Thus the export of this message is not complete. The message has to be checked and exported again.

Receive again

The inbox offers the function "Receive again". The respective message must be selected in the message browser. Use this function e. g. after a negative result of the check button. When trying to receive the message again, the application will ask the intermediary to send the respective message again.

Fetching new messages is done without further notice. The status is shown in the status section at the bottom of the P.O.box bar. You can see that message x of n is received and there will be a life indicator to show the finishing progress status.

A message after finishing is only shown, if something went wrong, e. g. the message is no longer available on the OSCI Manager and could not be restored. In this case a warning dialog is displayed that needs to be acknowledged. The menu option is the same as the one from the tool bar.

Note:

In case the message format of the received message does not conform to the defined format or it wasn't possible to encrypt the message completely, an error message is displayed. The message will be marked red in the inbox and the message status is undefined. The OSCI Manager will mark the message as "not yet collected". The message will neither be archived nor exported. Try to receive the message again. Please contact the support, if the message is replayed.

6.6.3 Handling messages

The following functions are assignable with the "Messages" menu as well as with the context menu or the function bar buttons.

6.6.3.1 Functions from the menu

Edit

Select any message in the outbox and select the "Edit" option. The button is disabled for forwarded or already signed messages. In the last case you have to remove all signatures before you are allowed to edit the note. The EGVP can only edit messages, which were created with the message dialog. Imported messages from a 3rd party application can only be deleted but not edited.

Check

Selecting this option initiates signature verification from the user interface. The option is not available in the archive. The verification of the message takes place in the background and the result is shown in the window "signature verification".

The verification result refers to mathematical integrity of the signed OSCI message according to the state it had when entering your file system. In case others may have manipulated the message on your file system the display in the administration window can differ from the originally received message. On verification the message is extracted from the signed OSCI message, which reverses possible modification that may have occurred in the meantime. A notification informs you about rebuilding a message. In case the system was not able to rebuild a manipulated OSCI message after verification it is marked red and an error notification is displayed. In order to detect the errors cause it should be selected and verified again.

Note:

A failed message verification may be due to manipulation. Proceed as follows: Mark the message in the inbox and click "receive again" or select "receive again" from the "message" menu. The message is fetched again from the OSCI Manager in its original state. Please mind that already fetched messages are only stored on the OSCI Manager for a certain period of time. Please ask your provider for information on storage duration.

If the verification is successful online certificate verification is executed automatically for the signed documents (PKCS#7, if existent). Therefore the user has to be online!

Please mind that signature verification only refers to the signed part of the message. The following parts of a message are not signed: Subject of the message, signature level, and local time.

If the status of a certificate according to the routing slip is not defined (yellow), it is verified again when the inspection sheet is created. In case the status has changed, this change is shown in the inspection sheet and the verification result is adjusted.

Sign

Using this option will open the dialog to select a private key for signing messages, which have to be signed with an advanced signature or do not require any signature. You can select either a software certificate or smartcard. In case the option "Yes, the private key is stored on a card" is selected you are asked to enter the signature PIN or to select the smartcard and enter the PIN afterwards. If "No, select a file with the key in a system, I am going to sign with the certificate stored in the file" is selected the explorer window will be displayed and you can select a p12 file (private key). After selecting a certificate the "Ciphering PIN-Entry" window is displayed and asks for the respective PIN.

For a qualified signature the dialog "PIN entry" or in case no smartcard is in the card reader the dialog "certificate selection" is shown. For the first case please enter the corresponding PIN. For the second case please put the smartcard into the card reader and select the certificate before entering the PIN.

Attention when sending messages to Germany:

For generating qualified digital signatures, only smartcard readers must be used that are confirmed according to the German Digital Signature Act (Deutsches Signaturgesetz, SigG) and whose confirmation is published by the Federal Network Agency (Bundesnetzagentur, BNetzA). With release of this application only the appointed smartcard readers met these requirements.

This application also supports smartcard readers that support insecure PIN entry or are not (yet) confirmed. If you use such a smartcard reader, don't use this application as a signature application component to create qualified digital signatures.

The message can be signed several times by running the function as often as needed. You can also sign more than one message at once when you have selected multiple messages in the outbox and use a software certificate. You only have to enter the PIN once and all messages are signed.

Remove signature(s)

This option removes signatures of a selected message from the outbox. If you want to remove one or more signatures a dialog opens where you can select the signature to be removed.

Import copy

By using this option you can copy one or more messages from a directory in the file system to the inbox. A dialog to select the message is displayed. This function also enables the import of stored messages to the P.O.box to use the verification functions of the EGVP.

Print

This function enables you to print a previously marked message. You can choose only one or several options and print them. After confirmation with "OK" the "Print" dialog will be displayed. The "Cancel" button will stop the function and "Help" will show the application's online help. The menu option is the same as the one from the tool bar. To print attachments you have to open the attachment first and print manually.

Delete

In all post boxes it is possible to mark one or a number of messages and choose the "Delete" option. Before a message is definitely deleted, you have to confirm the removal by clicking "Yes" in the upcoming Yes/No dialog. In case the message should not be deleted you can select "No". The menu option is the same as the one from the tool bar.

Forward

This function enables you to forward a previously marked message from your inbox. The address book opens and a new addressee has to be selected. Afterwards the message is saved in the outbox and all further functions are available. Only the data from the tabs "message", "business card", "attachments", and "content data" of the original message is forwarded.

Export

With this option a dialog opens and you can save one or more messages manually to the file system. With the button "select" define a directory to which the message is exported.

Note:

To enable the 3rd party application to notice when an export is finished the EGVP additionally creates a lock file `message.lock` within the export directory. The export by the EGVP is finished when the lock file is removed again.

3rd party import

To import 3rd party data the automated import function has to be active or the import has to be initiated manually (menu "import preferences/3rd party import"). The manual import can also be started by clicking on the "3rd party import" in the message menu. When the import is executed the message provided by the 3rd party application is converted into an OSCI message and stored in the outbox. In case problems occur during the import a second attempt is made by the EGVP.

After completing the 3rd party import the business data is shown in the outbox. The columns "Created", "Message type", "Subject", "Message-ID", "To", and "Signer" are displayed. The available tabs below are "Message", "Attachments" if present, "Content Data", and "Certificates". The message is marked as imported by a symbol. If the message was not imported correctly this symbol is displayed: . Now you can sign and send the created message.

6.6.3.2 Functions from the context menu

Functions are different in each post box (inbox, outbox and sentbox). Most of the functions that you can also find in the tool bar were already described in this chapter. In the following only functions will be described that are not available from the tool bar.

Mail to…

In all post boxes it is possible to send an e-mail with the message itself and the attachments and content data. When a message is marked and the function "Mail to…" is selected from the context menu, the respective e-mail program opens and a new e-mail message is created. The user has to enter the e-mail address and send the e-mail as usual. When forwarding the OSCI message all attachments, content data and HTML files generated by the EGVP are attached to the e-mail. The function is optimised for the Windows XP and the window manager "Gnome" under Linux.

Note:

This function uses a module that supports the following e-mail programs:

- Mozilla, Microsoft © Outlook and Microsoft © Outlook Express with Microsoft © Windows and
- Mozilla, Mozilla Thunderbird and Evolution with Linux

When using other e-mail programs the function "Mail to…" may not work properly.

Re-import

With the dynamic data transfer for business data messages, it can happen that content data or attachments cannot be imported properly due to several causes. To indicate this, these messages are marked red and with a different import symbol in the message area.

With the "Re-import" function, which is only applicable via the context menu, it is possible to repeat the respective import. This function is only available if loading of the delivered files failed.

Move

To move messages from the local archive to an archive data backup, mark the respective messages and select the context menu function "Move". This function is also available via the messages menu or with the shortcut Ctrl-M. Using this function will display the file explorer. The export folder defined in the "Export preferences" is displayed by default. Select a folder and save the selected messages into this directory. You can as well automate this function using the "Export preferences".

Restore

Accidentally deleted messages can be restored from the archive. For this purpose you can change to the archive, select the respective message, and execute the function "Restore" via the context menu or the messages menu. The message is restored in the inbox, the sentbox or in both.

Delete

Use the right mouse button to delete one or more messages.

Prove retrieval state

The first column in the sentbox indicates with an exclamation mark whether or not the message was retrieved from the addressee. The state of every single message is tested automatically when opening the post box and after that in a two hour interval.

You can mark one or several messages in the sentbox and start the prove-function with the context menu. The program then will ask the OSCI Manager for the current retrieval state and update the display in the user interface.

Open

From this menu within the tabs "attachments" and "content data" it is possible to open a file with the associated program. In case the file format is not linked to a program the file cannot be opened.

Extract and open the content of a PKCS#7 file

If the OSCI message contains signed files in PKCS#7 format as attachments these can be opened within the tabs "attachments" and "content data". The function is of special interest for PKCS#7 files, which were transferred in enveloping format. Opening the embedded document is only possible if the file type is part of the file name. Therefore the file name of the PKCS#7 file may not be changed. Example:

- file `name.doc.pkcs7`: extraction and opening is possible
- file `name.pkcs7`: extraction and opening is NOT possible

Save as

This function is available within the tabs "attachments" and "content data". It can be used to save attachments or content data to the file system.

Print

Print a file from the tabs "attachments" and "content data" from the associated program. In case the file format is not linked to a program the file cannot be printed. The function is optimised for Windows XP and Windows 2000.

If you experience any problems with printing from the context menu, check out the instructions in Appendix 1: How to fix problems with the print option in the context menu using Windows.

Subsequent verification of certificates

From the context menu each certificate can be verified by the OSCI Manager concerning its status (validity) Please mind that an active Internet connection is necessary. The result is displayed and can be saved or printed. A subsequent change of the results in the tab "inspection sheet" does not occur. For verification a time has to be defined. By default this is the time of entry on the server ("inbox" and "sentbox") or the time the message was created (outbox).

Details

Details can be viewed for every certificate by a right click.

6.7 Additional functions

In addition to the standard functions there are some more functions, which are described in the following:

6.7.1 Debug mode de-/activate

This function forces the application to log every activity within the post box until debugging is deactivated. You can deactivate the debug mode by selecting the menu item or closing the application. At this point an automatic e-mail with your default e-mail application is generated containing the logged information as attachment. The e-mail form asks for more information, which may be helpful to analyse the problem. Please answer these questions and send the e-mail to the stated addressee. The feature is optimised for Microsoft Windows XP and Windows 2000 and for Linux with the window manager "Gnome". Debug mode is active, when the lower right corner displays the text "You are in debug mode" and in the "Extras" menu the option "Debug mode" is checked.

Attention:

On 64-bit systems, the debug mode cannot be used. Please create e-mails with your e-mail client and add the logging output manually. In order to do this, please copy the content from the Java console. The console is shown by using the Java Control Panel (Tab "Advanced", Settings: Java Console).

Please send e-mails for supporting purposes to:

egvp@westernacher.de.

6.7.2 Re-enable disabled dialog boxes

With the help of "Re-enable disabled dialog boxes" in the "Options" menu all disabled message boxes are again displayed, as on first application launch.

6.7.3 Quit

From the menu "file" you can quit the application. In case there are still messages in the outbox you will receive a notification before the application is closed.

6.7.4 Agreement to changed privacy policy

In case the privacy policy has changed you will have to agree to the new privacy policy when opening your P.O.box before you can send and receive messages. If you disagree your address book entry is deleted from the directory service. Not yet received messages are

fetched. Creating new messages, sending, and receiving are not possible any more. You can now also delete the local P.O.box.

7 Reports

While receiving or sending messages several reports are produced. All reports assigned to a note are shown in the respective tab in the lower half of the application window. Please note that active tabs depend on the chosen post box. This chapter gives you information about the three possible reports.

Acknowledgement

This tab is only enabled in the sentbox and contains the data returned to sender from the OSCI Manager while sending. This data includes e. g. the timestamp when the message has entered the OSCI Manager. Additionally the name of the OSCI Manager, data about the sender and the signer of the particular message, information about the certificate and a listin of the transmitted attachments is shown.

Inspection sheet (HTML)

In the inbox the inspection sheet is available. This information was received together with the relevant message and contains the result of the signature and signature certificate verification performed by the OSCI Manager.

Signed attachments (HTML)

After receiving the OSCI message, the EGVP client automatically checks if signed attachments (PKCS#7) exist. The verification is executed for signed files stored in ZIP container as well. If signed attachments exist, EGVP tests the validity of all certificates used. For it, the application connects to the verification server (OCSP/CRL-Relay). The result of the validation is displayed in the additional tab "Signed attachments" and looks similar to the inspection sheet. The inspection sheet of signed attachments shows the format of PKCS#7 signatures:

- signature with document contents - for enveloping signatures
- signature without document contents - for detached signatures

If verification of signed attachments cannot be executed, it is documented in the inspection sheet for signed attachments. There are three possible error messages:

- An error occurred while trying to access the server.
- The signature's integrity could not be verified because of missing content data.
- The file <filename>.doc.pkcs7 could not be interpreted.

After finishing the validation of the signed attachments, the verification result of the message will be adjusted (first column in the inbox). The verification result is a summary of the validation results regarding the OSCI message and the inspection sheet of signed attachments. These are the rules:

- If one validation is "not valid" (red) the message status is set to "not valid" (red).

- If all validations are successful the message status is set to "valid" (green).
- If one validation is "not defined" (yellow) the message status is set to "not defined" (yellow)

If no signed attachment was sent the status of the inspection sheet applies.

	Note: Opening of an embedded document is only possible if the file type is included in the file name. The file name of the PKCS7 file may not be changed. (e. g. filename.doc.pkcs7)

Inspection sheet (XML)

In addition to the inspection sheet in HTML it is an inspection sheet in XML available. This inspection sheet shows the results of the verification of the signature and the verification of the certificate of the signature respective to the OSCI message. Furthermore if it is applicable it displays the results of the signed attachments. You will find the results in the message folder in the file system. By exporting a message the inspection sheet in XML will be exported as well. The inspection sheet in XML is available for the subsequent processing of a message due to a special application.

Result of the certificate verification

In the "certificates" tab the user can verify the certificate subsequently from the context menu. The result is shown in a separate window.

Transmission report

The transmission report is not shown in the application but can be selected from the function "print".

8 Explanations to the inspection sheet

Applied verifications

The OSCI Manager can perform different verification methods to verify an electronic signature enabling the user to act upon and to proceed with the message. The signature level and the particular certification authority (CA) define the complexity of the applied verification method. There is a difference between a signature check and the verification of the certificate used for signing. Checking the signature is done locally (e. g. on the receiver's computer). The verification of the certificate is performed online, if the related trust centre offers this service for this kind of certificate.

Mathematical signature verification

Before signing an electronic document, a so called hash value (or finger print) has to be created for the original message. Having a fixed length this value is a short document extract. Every file has its own hash value, so it is not possible to create a different file with the same hash value as the first one. This hash value will be encrypted with the sender’s private key. The original document, the signed hash value and the sender’s public key and certificate are sent to the receiver.

This is what the OSCI Manager does when checking the signature: First the encrypted hash value is decrypted with the sender's public key. The OSCI Manager computes a new hash value of the document and compares it with the hash value sent and signed by the signatures owner. If successful this ensures the integrity of the signed file but it does not mean that the certificate is valid and does not tell something about its quality and status.

Certificate verification

The verification of the signature certificate is executed to ensure that the certificates issuer (= trust centre) knows the identity of the person who signed, that the certificate is valid and not locked, and to ensure the authentication of the signature. The verification covers three steps:

- It creates a chain of certificates until it reaches the trusted anchor.
- All certificate signatures within the chain are checked cryptographically, regarding the validity of all used signature certificates and the certificates of their issuers at the moment of signing.
- Status verification of all certificates with different methods depending on the respective certification authority/trust centre.

The status verification is performed online requesting a trust centre. These are the validations supported by the OSCI Manager:

- OCSP (Online Certificate Status Protocol) verification with Common PKI: The trust centre returns the status of the certificate in question (valid and not locked, unknown or locked). E. g. the owner can get his certificate locked in case of loss.

- CRL (Certificate Revocation List) verification: Every issuer of certificates administrates a black list of locked certificates. The CRL verification will check that the respective black list does not contain the certificate in question.

- LDAP (Lightweight Directory Access protocol) verification: This validation will only ask the issuer if he knows the identity of the certificate.

To fit the requirements of the signature law for verification of qualified certificates, the OCSP verification or the combination of CRL and LDAP verification is recommended. Additionally the verification server (OCSP/CRL-Relay) tries to validate advanced certificates at trust centres in the same way, means if possibly with OCSP, else with the combination of CRL and LDAP verification.

Section "Summary and structure"

This is the primary part of the inspection sheet, containing the summary of all validations made.

- **Subject**: The OSCI subject within EGVP messages is defined as message type defined by author or sender.

- **Message-ID**: This unique ID is assigned by the OSCI Manager for referencing messages.

- **Sender**: This is the sender of the message as referred to in the business card.

- **Addressee:** This is the addressee of the message as referred to in certificate.

- **Entry at server**: Specifies the message's entry time on the server. This can be relevant for messages that have to adhere to a time limit. This statement also displays whether the given time OSCI Manager's server time or a timestamp of an accredited timestamp service provider.

- **Summarised verification state**: The message status is displayed. These are the possible states::

  - **All certificates were positively verified**. Further processing is possible without restrictions.

  - **At least one validation could not be executed**. The message's state is ambiguous. Please verify the information in section "Certificates and check results".

  - **At least one validation has the result not valid.** Thus the whole message is not legally binding. Further processing should not take place if liability is mandatory.

Further information is available in the document "Governikus-Pruefprotokoll.pdf" (only available in German).

9 Information about error messages and alerts

In case the information shown in the respective alert or error message does not help to fix the problem, please contact the support. Please use the debug mode to log details and assist the support to find a solution for you. Please refer to chapter "Debug mode de-/activate". Sometimes error messages contain incomprehensible source code. Please keep this code ready for the support employee.

This first section is about error messages in connection with an interrupted Internet connection, wrong network and proxy settings or an unavailable server. First of all please ensure that you have an active Internet connection. Furthermore you should check your network and proxy settings. If the check does not lead to any result please contact the support. The following error messages give you a hint that your Internet connection is interrupted, the network or proxy settings are not correct or a server is not available:

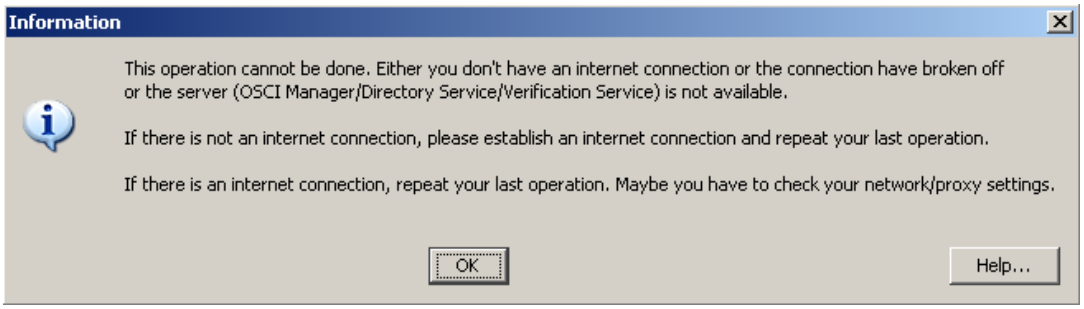
Information
This operation cannot be done. Either you don't have an internet connection or the connection have broken off or the server (OSCI Manager/Directory Service/Verification Service) is not available.
If there is not an internet connection, please establish an internet connection and repeat your last operation.
If there is an internet connection, repeat your last operation. Maybe you have to check your network/proxy settings.
OK
Help...

Figure 42: (Example) error message about proxy settings

In the right lower corner of the user interface two coloured symbols show that your Internet connection is interrupted or a server (directory service or OSCI Manager of the addressee) is not available at present (the colour changes from green to red when the sending failed and remains red until the sending was successful and the server is available again). A question mark indicates a not yet identified server status.

Example:

Figure 43: Server status

10 Table of figures

Figure 1: Java Control Panel of Java 6 16
Figure 2: Network settings 17
Figure 3: Java application runtime settings 17
Figure 4: Java Control Panel - Advanced 18
Figure 5: Java Web Start loads the application 19
Figure 6: Displaying the download status 19
Figure 7: Safety warning 20
Figure 8: Java terms of licence (example) 21
Figure 9: Terms of use 23
Figure 10: Select message folder 24
Figure 11: User interface (example) 25
Figure 12: Import a P.O. box 34
Figure 13: Setting in the tab "business card" 35
Figure 14: Settings in the tab "business card" 37
Figure 15: Create certificate and define PIN 39
Figure 16: Save certificate 39
Figure 17: PIN entry 40
Figure 18: Certificate display 40
Figure 19: Software certificate selection 41
Figure 20: Certificate selection dialog 41
Figure 21: PIN entry 42
Figure 22: Certificate read-out 43
Figure 23: Notification when using a smartcard for establishing a post box 43
Figure 24: Certificate display 44
Figure 25: Delete a P.O.box 46
Figure 26: Menu "Options" e-mail notification 48

Figure 27: Settings for e-mail notification....48
Figure 28: Menu "Options/Status report preferences"....49
Figure 29: Tab Interval of "Status report preferences" 49
Figure 30: Tab Notification of "Status report preferences" 50
Figure 31: Exchange certificate 51
Figure 32: Export settings, "inbox" tab....53
Figure 33: Export archived messages 54
Figure 34: Delete archived messages 55
Figure 35: Settings for automatic sending....56
Figure 36: Message window....60
Figure 37: Notification when trying to add a file with a non-accepted extension....62
Figure 38: Settings "Instant sending"....63
Figure 39: Address book - tab "Users" with example receivers....65
Figure 40: Details of the respective addressee....67
Figure 41: Selecting an addressee from the favourites tab....69
Figure 42: (Example) error message about proxy settings....85
Figure 43: Server status 85
Figure 44: Windows dialog "Folder Options”....88
Figure 45: Windows dialog "Edit File Type” 89
Figure 46: Windows dialog "Editing action”....89
Figure 47: Open the Java Control Panel and the Java Cache Viewer....90
Figure 48: The Java Cache Viewer 91

Appendix 1: How to fix problems with the print option in the context menu using Windows

If you have any problems printing from the context menu, the reason may be that there is no program defined for printing HTML files.

To fix this, follow these instructions:

1. Start Windows Explorer (e. g. by pressing Windows Key + E).
2. Select "Folder Options" from the "Tools" menu.
3. Choose the register "File Types".
4. Select HTML from the list "Registered file types" and click "Advanced".

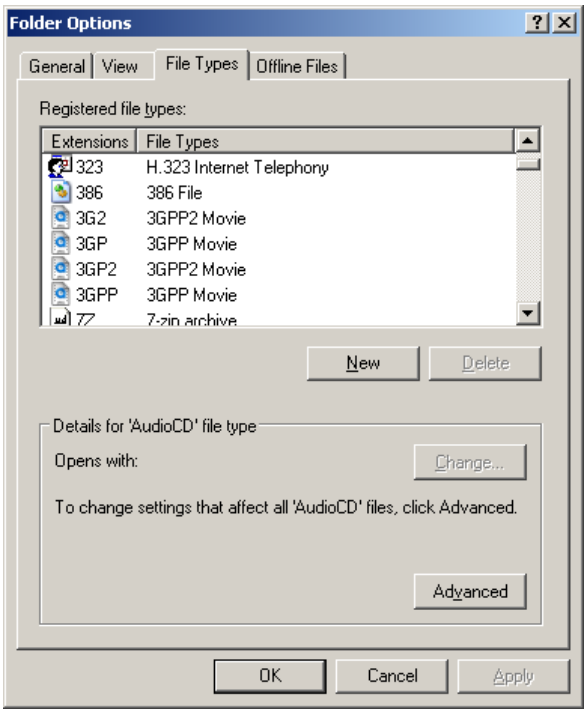

Figure 44: Windows dialog "Folder Options"

5. In the "Actions" list, select the entry "Print" and click "Edit". If there is no such entry, click "New" and enter "Print" in the "Action" text field.

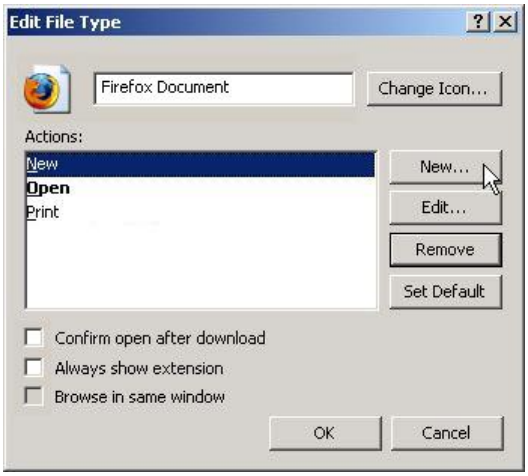

Figure 45: Windows dialog "Edit File Type”

6. Enter the following line in the "Application used to perform action” text field:

   ```
   rundll32.exe C:\WINDOWS\System32\mshtml.dll,PrintHTML "%1"
   ```

   In case Windows is not installed in C:\Windows, please alter the path accordingly.

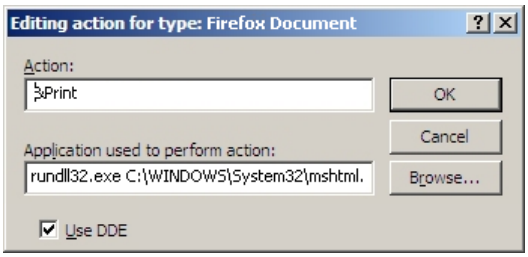

Figure 46: Windows dialog "Editing action”

7. Close all opened dialogs by clicking OK.

8. If the problem is not fixed after a reboot, change the entry in the "Action" text field from "Print" to "printto".

Appendix 2: How to uninstall the EGVP application

In case the use of the installer is required, it is recommended to uninstall already existing JNLP EGVP applications with the help of the Java Control Panel. To uninstall a Java application the Java Cache Viewer has to be started with the help of the Java Control Panel.

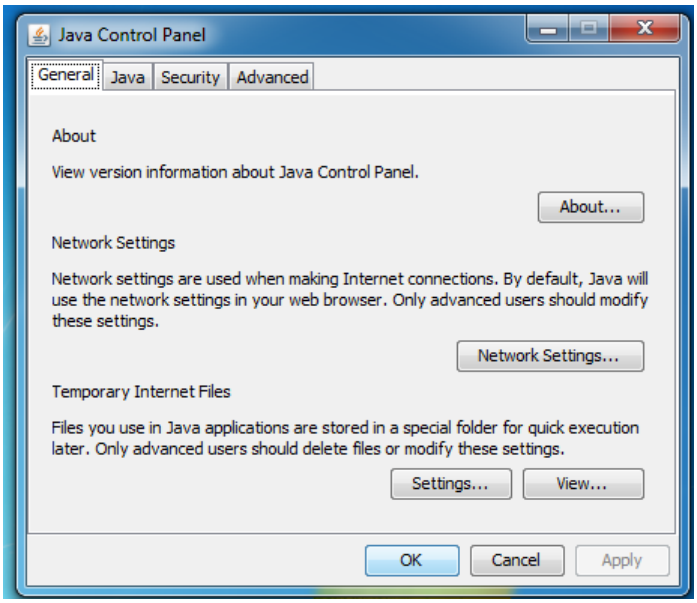
Java Control Panel
General
Java
Security
Advanced
About
View version information about Java Control Panel.
About...
Network Settings
Network settings are used when making Internet connections. By default, Java will use the network settings in your web browser. Only advanced users should modify these settings.
Network Settings...
Temporary Internet Files
Files you use in Java applications are stored in a special folder for quick execution later. Only advanced users should delete files or modify these settings.
Settings...
View...
OK
Cancel
Apply

Figure 47: Open the Java Control Panel and the Java Cache Viewer

Windows:

1. Open the windows control panel,
2. Double click the Java button to open the Java Control Panel,
3. Select the "General" tab;
4. Click the button "View" to open the Java Cache Viewer dialog.

Linux:

1. Launch the command-line interface or press Alt-F2,
2. Enter javaws - viewer and press enter to open the Java Cache Viewer dialog.

Mark the respective application and click the red cross above.

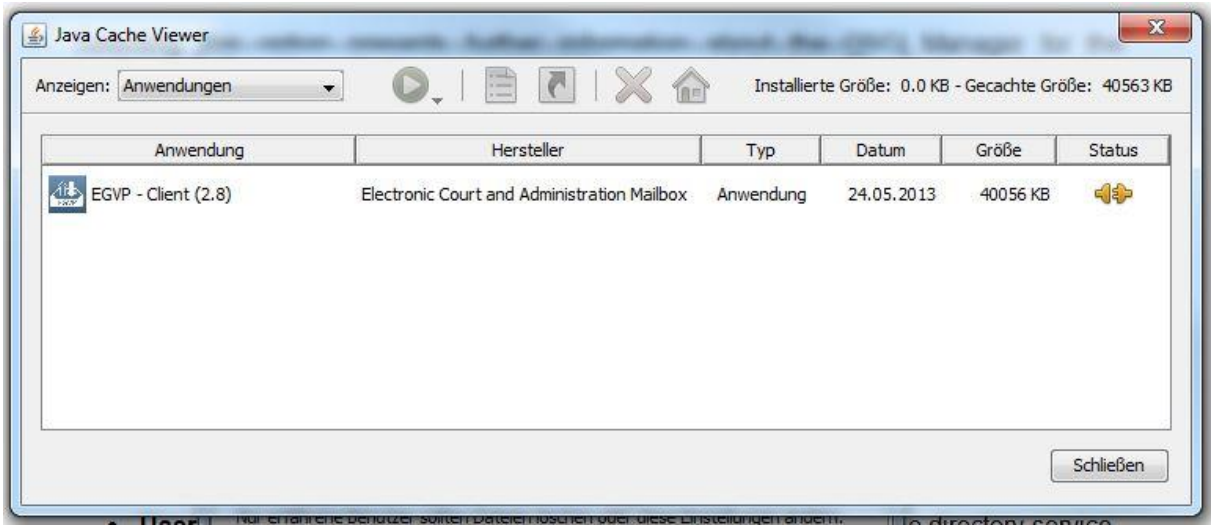

Figure 48: The Java Cache Viewer

The uninstalled application can be found in the Deleted Applications tab (dropdown upper left corner). Possibly existing desktop or menu entries for the Java application are deleted as well.